INTRODUCCIÓN A LA

# TEORÍA DE LOS NÚMEROS

NIVEN Y
ZUCKERMAN

LIMUSA

**IVAN NIVEN** recibió su Doctorado en Matemáticas en la Universidad de Chicago en 1938. Actualmente es profesor de matemáticas de la Universidad de Oregon, Eugene, Oregon.

**HERBERT S. ZUCKERMAN** se doctoró en matemáticas en la Universidad de California, Berkeley, en 1936. En la actualidad es profesor de matemáticas de la Universidad de Washington, Seattle, Washington.

# INTRODUCCION A LA TEORIA DE LOS NUMEROS

# INTRODUCCION A LA TEORIA DE LOS NUMEROS

**IVAN NIVEN**
*Universidad de Oregon*

**HERBERT S. ZUCKERMAN**
*Universidad de Washington*



**EDITORIAL LIMUSA**
**MEXICO** **1976**

# INTRODUCCION A LA TEORIA DE LOS NUMEROS

**IVAN NIVEN**
*Universidad de Oregon*

**HERBERT S. ZUCKERMAN**
*Universidad de Washington*



EDITORIAL LIMUSA
MEXICO 1976

Versión autorizada en español de la 2a. edición original en inglés, publicada por John Wiley & Sons, Inc., Nueva York, bajo el título: AN INTRODUCTION TO THE THEORY OF NUMBERS.



Versión española:

JOSE HERNAN PEREZ CASTELLANOS

Ingeniero Industrial, Profesor Titular de
Matemáticas de la Escuela Superior de
Ingeniería Mecánica y Eléctrica del
Instituto Politécnico Nacional de México.

Revisión:

JAVIER GONZALEZ GARZA

Maestría en Matemáticas del Centro de
Investigación y Estudios Avanzados del
Instituto Politécnico Nacional de México.
Profesor de Matemáticas de la Escuela Superior
de Física y Matemáticas del Instituto
Politécnico Nacional de México.


Arcos de Belén 75, México 1, D. F.
Miembro de la Cámara Nacional de la
Industria Editorial. Registro Núm. 121

Primera edición: 1969

***Primera reimpresión: 1976***

*Impreso en México*

(1866)

# Prólogo

Esta edición ha sido notablemente enriquecida con explicaciones más precisas en varios de sus capítulos, fundamentalmente en los de introducción y sobre conceptos básicos. Se ha puesto especial atención a los pasos de transición de los problemas fáciles hacia los difíciles, así como en otros aspectos que, tal vez, no estaban suficientemente claros en la primera edición de la obra en inglés.

Los autores expresan su agradecimiento a Paul T. Bateman, Charles W. Curtis, Emma Lehmer y Sigmund Selberg por sus útiles sugestiones. Agradecemos a John Wiley & Sons su amable consideración por complacer nuestros deseos respecto al formato y la tipografía.

*Marzo 1966*

# Prólogo a la primera edición

Nuestro propósito ha sido presentar una introducción a la teoría de los números lo más completa posible, dentro de los límites que señala un volumen tan breve. Los conceptos básicos se exponen en la primera parte del libro, y a continuación está el material más especializado en los tres capítulos finales. Para establecer la semejanza con el desarrollo que procede de los tópicos generales a los estudios más particulares, hemos tratado de empezar el libro a un ritmo más lento que el usado posteriormente. Por tanto, las últimas partes del libro se presentan en forma más compacta y elaborada que las primeras.

El libro se ha escrito para estudiantes del último año de profesional de centros de estudios superiores. Contiene por lo menos suficiente material para impartir un curso de un año y es posible desarrollar un curso breve mediante el uso de las secciones 1.1 a 1.3; 2.1 a 2.4; 3.1, 3.2, 4.1; 5.1 a 5.3; 5.5, 6.1 y 6.2. Pueden hacerse otros arreglos porque, salvo algunas excepciones, los capítulos posteriores al cuarto son independientes entre sí y especialmente los tres capítulos finales.

A fin de que el estudiante profundice sus conocimientos de la materia, hemos proporcionado un número considerable de problemas. Estos ejercicios son de amplia variedad, yendo de los simples problemas numéricos hasta desarrollos adicionales de la teoría. El principiante en el estudio de la teoría de los números debe saber que la materia se distingue por la dificultad de sus problemas, y muchos problemas que parecen simples por su planteamiento, indican muy poca de la gran habilidad o perspicacia que requiere su solución. Como es de esperar, los problemas más difíciles se colocaron al final de cada grupo de ejercicios. En muchos casos, tres o cuatro problemas consecutivos constituyen una serie conexa en la cual los últimos pueden resolverse más fácilmente mediante la aplicación de la información obtenida en los primeros. Como norma, hemos hecho el texto completamente independiente de los problemas, y en ninguna parte, la demostración de un teorema depende de los resultados de cualquier problema.

Al escoger los métodos de demostración, tratamos de incluir tantos como ha sido posible. Procuramos establecer las demostraciones con exactitud, evitando proposiciones que resulten también engañosas y eludiendo análisis excesivamente largos de detalles sin importancia. Conforme el lector progrese, se familiarizará cada vez con más métodos y será capaz de plantear demostraciones exactas siguiendo el modelo de las muestras.

El lector que se interese en ampliar sus conocimientos sobre la materia encontrará muy útil la bibliografía que está al final del libro. En particular, quienes se interesen en la historia de este tema, pueden consultar el libro *Number Theory and Its History,* de O. Ore y, para información más específica, la obra titulada *History of the Theory of Numbers,* de L. E. Dickson. Nuestro enfoque es analítico, no histórico, y no intentemos atribuir a sus descubridores originales varios teoremas y demostraciones. No obstante, deseamos puntualizar que aceptamos la sugestión de Peter Scherk respecto a que usaremos el planteamiento de F. J. Dyson de la demostración del Teorema $\alpha\beta$ de Mann. Nuestra demostración se basa en las notas que Peter Scherk nos proporcionó amablemente. Les agradecemos a los editores del *American Mathematical Monthly* por permitirnos usar algunos problemas. También apreciamos la cuidadosa lectura del manuscrito efectuada por Margaret Maxfield, cuyos esfuerzos lo mejoraron notablemente. Finalmente, quisiéramos manifestar nuestro profundo aprecio y amplio reconocimiento a los matemáticos L. E. Dickson, R. D. James, D. N. Lehmer y Hans Rademacher, cuyas conferencias nos fueron vitales para iniciar la teoría de los números.

IVAN NIVEN
*Junio 1960* HERBERT S. ZUCKERMAN

# Contenido

# Capítulo 1

# Divisibilidad

## 1.1 Introducción

La teoría de los números está relacionada primordialmente con las propiedades de los números naturales, 1, 2, 3, 4, . . . , también llamados enteros positivos. Sin embargo, la teoría no se confina estrictamente a los números naturales ni aun al conjunto de todos los enteros: 0, $\pm$ 1, $\pm$ 2, $\pm$ 3, . . . . De hecho, algunos teoremas de la teoría de los números se prueban más fácilmente haciendo uso de las propiedades de los números reales o de los complejos, aunque la proposición de los teoremas se refiera únicamente a los números naturales. Asimismo, existen teoremas relacionados con los números reales que dependen en tal forma de las propiedades de los enteros que con toda propiedad se incluyen en la teoría de los números.

Se dice que un entero $n$ mayor que 1 es primo si no tiene divisor $d$ tal que $1 < d < n$. El hecho de que para todo entero positivo $m$ dado existe un primo mayor que $m$ se establece en términos de los enteros y puede probarse a partir de las propiedades de los números naturales exclusivamente. El hecho de que todo número natural puede expresarse como una suma de, cuando más, cincuenta y cuatro quintas potencias de los enteros, también se establece en términos de los números naturales, pero cualquier demostración conocida depende de las propiedades de los números complejos. Finalmente, la cuestión de cuántos primos existen, tales que no sean mayores que $x$, evidentemente pertenece a la teoría de los números, pero su respuesta contiene la función $\log x$ y está bastante fuera del dominio de los números naturales. Los dos ejemplos

últimos están más allá del alcance de este libro. Sin embargo, no nos restringiremos a los enteros, sino que, usaremos los números reales y los complejos cuando sea conveniente. Los asuntos discutidos en este libro no son cálculos o curiosidades numéricas, excepto en el caso en que éstos sean de importancia para las proposiciones generales. Tampoco discutiremos los fundamentos del sistema numérico; se supone que el lector está familiarizado no sólo con los enteros, sino también con los números racionales y reales. No obstante, para abordar el estudio de la teoría de los números no es requisito un riguroso análisis lógico del sistema de los números reales.

La teoría de los números cuenta, para sus demostraciones, con un gran número de ideas y métodos. De éstos, existen dos principios básicos a los cuales les dedicaremos atención especial. El primero es que cualquier conjunto de enteros positivos tiene un elemento menor si contiene a cualquiera de los miembros. En otras palabras, si un conjunto $S$ de enteros positivos no es vacío, entonces contiene un entero $s$ tal, que para cualquier miembro $a$ de $S$, se cumple la relación $s \leqq a$. El segundo principio, inducción matemática, es una consecuencia lógica del primero,* el cual puede establecerse de la manera siguiente: si un conjunto $S$ de enteros positivos contiene al entero 1, y contiene a $n + 1$ siempre que contenga a $n$, entonces $S$ consiste de todos los enteros positivos.

Tal vez sea conveniente puntualizar que una aseveración negativa como, por ejemplo, "No todo entero positivo puede expresarse como una suma de los cuadrados de tres enteros", solamente requiere que se produzca un ejemplo, el número 7 no puede expresarse así. Por otra parte, una aseveración positiva tal como "todo entero positivo puede expresarse como una suma de los cuadrados de cuatro enteros", no puede probarse mediante ejemplos, aunque sean numerosos. Este resultado es el del Teorema 5.6 en el capítulo 5, donde se proporciona una demostración.

Finalmente, se supone que el lector está familiarizado con la forma acostumbrada de las proposiciones matemáticas. En particular, si $A$ denota alguna aseveración o bien una colección de aseveraciones, lo mismo que $B$, las proposiciones siguientes son lógicamente equivalentes —únicamente son formas diferentes de decir la misma cosa.

$A$ implica $B$.
Si $A$ es verdadera, entonces $B$ es verdadera.
Para que $A$ sea verdadera es necesario que $B$ sea verdadera.
$B$ es una condición necesaria para $A$.
$A$ es una condición suficiente para $B$.

* Consultar *A Survey of Modern Algebra* de G. Birkhoff y S. MacLane, edición revisada, Macmillan, 1953, pp. 10-13.

Si $A$ implica $B$ y $B$ implica $A$, entonces puede decirse que $B$ es una condición necesaria y suficiente para que se cumpla $A$.

En general, usaremos letras del alfabeto romano, $a, b, c, \ldots, m, n, \ldots, x, y, z$, para designar a los enteros, a menos que se especifique otra cosa.

## 1.2 Divisibilidad

**Definición 1.1** *Un entero $b$ es divisible por un entero $a$, no cero, si existe un entero $x$ tal que $b = ax$ y se escribe $a|b$. En el caso en que $b$ no sea divisible por $a$ se escribe $a \nmid b$.*

Otra manera de expresar la propiedad de divisibilidad $a|b$, es decir, que $a$ divide a $b$, que $a$ es un divisor de $b$ y, que $b$ es un múltiplo de $a$. Si $a|b$ y $0 < a < b$, entonces $a$ es un divisor propio de $b$. Se entiende que nunca se usará 0 como el miembro izquierdo del par de enteros en $a|b$. Por otra parte, no solamente puede tenerse 0 como el miembro derecho del par, sino que, también, en tales casos siempre tendremos divisibilidad. Así, $a|0$ para todo entero $a$ diferente de cero. En ocasiones se usa la notación $a^K \| b$ para indicar que $a^K|b$ pero $a^{K+1} \nmid b$.

**Teorema 1.1**

(1) *$a|b$ implica $a|bc$ para cualquier entero $c$;*
(2) *$a|b$ y $b|c$ implica $a|c$;*
(3) *$a|b$ y $a|c$ implica $a|(bx + cy)$ para cualesquiera enteros $x$ y $y$;*
(4) *$a|b$ y $b|a$ implica $a = \pm b$;*
(5) *$a|b$, $a > 0$, $b > 0$, implica $a \leqq b$.*

*Demostración.* Las demostraciones de estos resultados se deducen inmediatamente a partir de la definición de divisibilidad. La propiedad 3 admite una obvia extensión para cualquier conjunto finito, así:

$$a|b_1, b|b_2, \cdots, a|b_n \text{ implica } a \left| \sum_{j=1}^{n} b_j x_j \right. \text{ para cualesquiera enteros } x_j.$$

La propiedad 2 puede extenderse de manera semejante.

**Teorema 1.2** *El algoritmo de la división. Dados dos enteros cualesquiera $a$ y $b$, con $a > 0$, existen los enteros $q$ y $r$ tales que $b = qa + r$, $0 \leqq r < a$. Si $a \nmid b$, entonces $r$ satisface las desigualdades más fuertes $0 < r < a$.*

*Demostración. Considérese la progresión aritmética*

$$\ldots, b - 3a, b - 2a, b - a, b, b + a, b + 2a, b + 3a, \ldots$$

extendiéndose indefinidamente en ambas direcciones. En esta sucesión, selecciónese el miembro no negativo menor y denótese por $r$. Por tanto, por definición, $r$ satisface las desigualdades del teorema. Pero también $r$, estando en la sucesión, es de la forma $b - qa$ y así $q$ está definido en términos de $r$, y se complementa la demostración.

Se ha establecido el teorema con la suposición de que $a > 0$. Sin embargo, esta hipótesis no es necesaria y puede formularse el teorema sin ella: dados dos enteros cualesquiera $a$ y $b$, con $a \neq 0$, existen los enteros $q$ y $r$ tales que $b = qa + r$, $0 \leqq r < |a|$.

El Teorema 1.2 recibe el nombre de algoritmo de la división. Un algoritmo es un procedimiento o método matemático para obtener un resultado. Se ha establecido el Teorema 1.2 en la forma "existen los enteros $q$ y $r$" y esta expresión sugiere que tenemos el llamado teorema de existencia en lugar de un algoritmo. No obstante, puede observarse que la demostración proporciona un método para obtener los enteros $q$ y $r$, puesto que solamente es necesario examinar en parte la progresión aritmética infinita $\ldots, b - a, b, b + a, \ldots$ para obtener el miembro positivo menor $r$.

En la práctica, el cociente $q$ y el residuo $r$ se obtienen mediante la división aritmética de $a$ entre $b$.

**Definición 1.2** *El entero $a$ es un* divisor común *de $b$ y $c$ en el caso de que $a|b$ y $a|c$. Puesto que solamente existe un número finito de divisores de cualquier entero diferente de cero, solamente existen un número finito de divisores comunes de $b$ y $c$, excepto en el caso de que $b = c = 0$. Si por lo menos uno de $b$ y $c$ no es 0, el mayor entre sus divisores comunes se llaman* máximo común divisor *de $b$ y $c$ y se denota por $(b, c)$. De modo semejante se denota el máximo común divisor $g$ de los enteros $b_1, b_2, \ldots, b_n$, no todos cero, por $(b_1, b_2, \ldots, b_n)$.*

Por tanto, el máximo común divisor $(b, c)$ está definido para todo par de enteros $b, c$ excepto $b = 0$, $c = 0$ y se observa que $(b, c) \geqq 1$.

**Teorema 1.3** *Si $g$ es el máximo común divisor de $b$ y $c$, entonces existen los enteros $x_0$ e $y_0$ tales que $g = (b, c) = bx_0 + cy_0$.*

*Demostración.* Considérense las combinaciones lineales $bx + cy$, donde $x$ y $y$ recorren todos los enteros. Este conjunto de enteros $\{bx + cy\}$ incluye valores positivos y negativos, y también 0 seleccionando $x = y = 0$. Escójanse $x_0$ y $y_0$ de manera que $bx_0 + cy_0$ sea el menor entero positivo $l$ en el conjunto; así que $l = bx_0 + cy_0$.

En seguida se probará que $l|b$ y $l|c$. Se establecerá la primera propiedad, la segunda se deduce por analogía. Se dará una demostración indirecta de que $l|b$, esto es, se supone que $l \nmid b$ y se obtiene una contradicción. A

partir de que $l \nmid b$ se deduce que existen los enteros $q$ y $r$, por el Teorema 1.2, tales que $b = lq + r$ con $0 < r < l$. De aquí que se tiene $r = b - lq = b - q(bx_0 + cy_0) = b(l - qx_0) + c(-qy_0)$ y, por tanto, $r$ está en el conjunto $\{bx + cy\}$. Esto contradice el hecho de que $l$ es el menor entero positivo en el conjunto $\{bx + cy\}$.

Ahora, puesto que $g$ es el máximo común divisor de $b$ y $c$, puede escribirse $b = gB$, $c = gC$ y $l = bx_0 + cy_0 = g(Bx_0 + Cy_0)$. De donde $g|l$, y así, por la parte 5 del teorema 1.1, se concluye que $g \leqq l$. Ahora bien, $g < l$ es imposible, supuesto que $g$ es el *máximo* común divisor y, por tanto, $g = l = bx_0 + cy_0$.

**Teorema 1.4** *El máximo común divisor $g$ de $b$ y $c$ puede caracterizarse en las dos formas siguientes:* (1) *es el menor valor positivo de $bx + cy$ donde $x$ y $y$ recorren todos los enteros;* (2) *es el común divisor positivo de $b$ y $c$ el cual es divisible entre cada divisor común.*

*Demostración.* La parte 1 se concluye a partir de la demostración del Teorema 1.3. Para probar la parte 2, obsérvese que si $d$ es cualquier divisor común de $b$ y $c$, entonces $d|g$ por la parte 3 del Teorema 1.1. Además, no pueden existir dos enteros distintos con la propiedad 2, debido al Teorema 1.1, parte 5.

**Teorema 1.5** *Dados los enteros cualesquiera $b_1, b_2, \ldots, b_n$ no todos cero, con máximo común divisor $g$, existen los enteros $x_1, x_2, \cdots, x_n$ tales que*

$$g = (b_1, b_2, \cdots, b_n) = \sum_{j=1}^{n} b_j x_j.$$

*Además, $g$ es el menor valor positivo de la forma lineal $\sum_{j=1}^{n} b_j y_j$ donde* los $y_j$ *recorren todos los enteros; también $g$ es el divisor común positivo de $b_1, b_2, \ldots, b_n$ el cual es divisible entre cada divisor común.*

*Demostración.* Este resultado es una generalización directa de los dos teoremas precedentes y la demostración es análoga sin complicaciones debido al paso de dos enteros a $n$ enteros.

**Teorema 1.6** *Para cualquier entero positivo $m$,*

$$(ma, mb) = m(a, b).$$

*Demostración.* Por el Teorema 1.4 se tiene

$$\begin{aligned}(ma, mb) &= \text{menor valor positivo de } max + mby \\ &= m \cdot \{\text{menor valor positivo de } ax + by\} \\ &= m(a, b).\end{aligned}$$

**Teorema 1.7** *Si* $d|a$ *y* $d|b$ *y* $d > 0$, *entonces*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b).$$

*Si* $(a, b) = g$, *entonces* $$\left(\frac{a}{g}, \frac{b}{g}\right) = 1.$$

*Demostración.* La segunda aseveración es el caso especial de la primera obtenida al usar el máximo común divisor $g$ de $a$ y $b$ en el papel de $d$. A su vez, la primera aseveración, es una consecuencia directa del Teorema 1.6 obtenida al reemplazar $m, a, b$ en ese teorema por $d$, $(a/d)$, $(b/d)$, respectivamente.

**Teorema 1.8** *Si* $(a, m) = (b, m) = 1$, *entonces* $(ab, m) = 1$.

*Demostración.* Por el Teorema 1.3, existen los enteros $x_0$, $y_0$, $x_1$, $y_1$ tales que $1 = ax_0 + my_0 = bx_1 + my_1$. Por tanto, puede escribirse $(ax_0)(bx_1) = (1 - my_0)(1 - my_1) = 1 - my_2$ donde $y_2$ está definido por la ecuación $y_2 = y_0 + y_1 - my_0y_1$. De la ecuación $abx_0x_1 + my_2 = 1$ se observa, por la parte 3 del Teorema 1.1, que cualquier divisor común de $ab$ y $m$ es un divisor de 1 y de aquí que $(ab, m) = 1$.

**Definición 1.3** *Se dice que* $a$ *y* $b$ *son* primos relativos *en el caso de que* $(a, b) = 1$, *y que* $a_1, a_2, \cdots, a_n$ *son* primos relativos *en el caso de que* $(a_1, a_2 \cdots, a_n) = 1$. *Se dice que* $a_1, a_2, \cdots, a_n$ *son* primos relativos en pares *en el caso de que* $(a_i, a_j) = 1$ *para todo* $i = 1, 2, \cdots, n$ *y* $j = 1, 2, \cdots, n$ *con* $i \neq j$.

El hecho de que $(a, b) = 1$ en ocasiones se expresa diciendo que $a$ y $b$ son coprimos o bien diciendo que $a$ es primo para $b$.

**Teorema 1.9** *Para todo* $x$, $(a, b) = (b, a) = (a, -b) = (a, b + ax)$.

*Demostración.* Denótese $(a, b)$ por $d$ y $(a, b + ax)$ por $g$. Es evidente que $(b, a) = (a, -b) = d$.

Por aplicación del Teorema 1.1, partes 3 y 4, se obtiene $d|g$, $g|d$ y de aquí que $d = g$.

**Teorema 1.10** *Si* $c|ab$ *y* $(b, c) = 1$, *entonces* $c|a$.

*Demostración.* Por el Teorema 1.6, $(ab, ac) = a(b, c) = a$. Pero $c|ab$ y $c|ac$, de donde, por el Teorema 1.4, $c|a$.

Dados dos enteros $b$ y $c$, ¿cómo puede encontrarse el máximo común divisor $g$? La Definición 1.2 no responde a esta pregunta, ni el Teorema 1.3 el cual simplemente asegura la existencia de un par de enteros $x_0$ y $y_0$ tales que $g = ax_0 + by_0$. Si $b$ y $c$ son pequeños, los valores de

$g$, $x_0$ y $y_0$ pueden encontrarse por inspección. Por ejemplo, si $b = 10$ y $c = 6$, es obvio que $g = 2$, y un par de valores para $x_0$, $y_0$ es 2, $-3$. A continuación estableceremos un algoritmo que proporciona un método general para encontrar el valor de $g$ y también los valores de $x_0$ y $y_0$. Por el Teorema 1.9, $(b, c) = (b, -c)$ y de aquí que puede suponerse $c$ positivo, puesto que el caso $c = 0$ es muy especial: $(b, 0) = |b|$.

**Teorema 1.11** *El algoritmo euclidiano. Dados los enteros $b$ y $c > 0$, se hace una aplicación repetida del algoritmo de la división, Teorema* 1.2, *para obtener una serie de ecuaciones*

$$\begin{aligned}
b &= cq_1 + r_1, & 0 &< r_1 < c,\\
c &= r_1q_2 + r_2, & 0 &< r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, & 0 &< r_3 < r_2,\\
&\cdots & &\cdots\\
r_{j-2} &= r_{j-1}q_j + r_j, & 0 &< r_j < r_{j-1},\\
r_{j-1} &= r_jq_{j+1}.
\end{aligned}$$

*El máximo común divisor $(b, c)$ de $b$ y $c$ es $r_j$, el último residuo diferente de cero en el proceso de la división. Los valores de $x_0$ y $y_0$ en $(b, c) = bx_0 + cy_0$ pueden obtenerse eliminando $r_1, r_2, \ldots, r_{j-1}$ en el conjunto de ecuaciones.*

**Ejemplo.** $b = 963$, $c = 657$.

$$\begin{aligned}
963 &= 657 \cdot 1 + 306\\
657 &= 306 \cdot 2 + 45\\
306 &= 45 \cdot 6 + 36\\
45 &= 36 \cdot 1 + 9\\
36 &= 9 \cdot 4
\end{aligned}$$

Por tanto $(963, 657) = 9$, y 9 puede expresarse como una combinación lineal de 963 y 657 eliminando los residuos 36, 45 y 306, de la manera siguiente:

$$\begin{aligned}
9 &= 45 - 36\\
&= 45 - (306 - 45 \cdot 6)\\
&= -306 + 7 \cdot 45\\
&= -306 + 7(657 - 306 \cdot 2)\\
&= 7 \cdot 657 - 15 \cdot 306\\
&= 7 \cdot 657 - 15(963 - 657)\\
&= 22 \cdot 657 - 15 \cdot 963.
\end{aligned}$$

*Demostración.* La cadena de ecuaciones se obtiene dividiendo $c$ entre $b$, $r_1$, entre $c$, $r_2$ entre $r_1, \ldots, r_j$ entre $r_{j-1}$. El proceso se detiene cuando la división es exacta, es decir cuando el residuo es cero. Así que,

en nuestra aplicación del Teorema 1.2 hemos escrito las desigualdades para el residuo sin un signo de igualdad, por ejemplo, $0 < r_1 < c$ en lugar de $0 \leqq r_1 < c$, porque si $r_1$ fuera igual a cero, la cadena se terminaría en la primera ecuación $b = cq_1$ en cuyo caso el máximo común divisor de $b$ y $c$ sería $c$.

Ahora se probará que $r_j$ es el máximo común divisor $g$ de $b$ y $c$. Supuesto que $g|b$ y $g|c$, se ve que $g|r_1$ por la primera ecuación de la cadena. Puesto que $g|c$ y $g|r_1$, se ve que $g|r_2$ por la segunda ecuación. Continuando mediante inducción matemática se encuentra que $g|r_j$. Por otra parte, la ecuación final implica que $r_j|r_{j-1}$. Esto, junto con la penúltima ecuación, implica $r_j|r_{j-2}$. Continuando mediante inducción matemática se concluye que $r_j|b$ y $r_j|c$. Por el Teorema 1.4, $r_j|g$. De aquí que $g = r_j$ por el Teorema 1.1.

Para ver que $r_j$ se expresa como una combinación de $b$ y $c$, simplemente se necesita eliminar $r_1$ mediante las dos primeras ecuaciones de la cadena, a continuación eliminar $r_2$ entre la ecuación resultante y la tercera. Procediendo con las eliminaciones sucesivas de $r_3, r_4, \cdots, r_{j-1}$, se obtiene $r_j$ en la forma $bx_0 + cy_0$.

**Definición 1.4** *Los enteros $a_1, a_2, \cdots, a_n$ todos diferentes de cero, tienen un* múltiplo común *$b$ si $a_i|b$ para $i = 1, 2, \cdots, n$. (Nótese que existen múltiplos comunes; por ejemplo, el producto $a_1 a_2 \cdots, a_n$ es uno). El menor de los múltiplos comunes positivos recibe el nombre de mínimo común múltiplo y se denota por $[a_1, a_2, \cdots, a_n]$.*

**Teorema 1.12** *Si $b$ es cualquier múltiplo común de $a_1, a_2, \cdots, a_n$, entonces $[a_1, a_2, \cdots, a_n]|b$. Esto equivale a decir que si $h$ denota a $[a_1, a_2, \cdots, a_n]$, entonces $0, \pm h, \pm 2h, \pm 3h, \cdots$ incluyen todos los múltiplos comunes de $a_1, a_2, \cdots, a_n$.*

*Demostración.* Sea $m$ cualquier múltiplo común, divídase $m$ entre $h$. Por el Teorema 1.2, existen un cociente $q$ y un residuo $r$, tales que, $m = qh + r$, $0 \leqq r < h$. Debe probarse que $r = 0$. Si $r \neq 0$ se argumenta del modo siguiente. Para cada $i = 1, 2, \cdots, n$ se sabe que $a_i|h$ y $a_i|m$, de modo que $a_i|r$. Así que, $r$ es un múltiplo común positivo de $a_1, a_2, \cdots, a_n$ contrario al hecho de que $h$ es el menor positivo de todos los múltiplos comunes.

**Teorema 1.13** *Si $m > 0$, $[ma, mb] = m[a, b]$.* También $[a, b] \cdot (a, b) = |ab|$.

*Demostración.* Ya que $[ma, mb]$ es un múltiplo de $ma$, *a fortiori* es un múltiplo de $m$ y, por tanto, puede escribirse en la forma $mh_1$. Denotando $[a, b]$ por $h_2$, se oberva que $a|h_2$, $b|h_2$, $am|mh_2$, $bm|mh_2$ y, por el Teorema 1.12, $mh_1|mh_2$. De donde $h_1|h_2$. Por otra parte, $am|mh_1$,

$bm|mh_1$, $a|h_1$, $b|h_1$ y así $h_2|h_1$. Se concluye que $h_1 = h_2$ y así se establece la primera parte del teorema.

Será suficiente probar la segunda parte para los enteros positivos $a$ y $b$, puesto que $[a, -b] = [a, b]$. Empecemos con el caso especial donde $(a, b) = 1$. Ahora bien, $[a, b]$ es un múltiplo de $a$, digamos $ma$. Entonces $b|ma$ y $(a, b) = 1$, así que por el Teorema 1.10 se concluye que $b|m$. De aquí que $b \leqq m$, $ba \leqq ma$. Pero $ba$, siendo un múltiplo común positivo de $b$ y $a$, no puede ser menor que el mínimo común múltiplo y, por tanto, $ba = ma = [a, b]$.

Regresando al caso general, donde $(a, b) = g > 1$, se tiene $((a/g), (b, g)) = 1$, por el Teorema 1.7. Al aplicar el resultado del párrafo precedente, se obtiene

$$\left[\frac{a}{g}, \frac{b}{g}\right]\left(\frac{a}{g}, \frac{b}{g}\right) = \frac{a}{g}\frac{b}{g}.$$

Al multiplicarse por $g^2$ y usando el Teorema 1.6 así como la primera parte del presente teorema, se obtiene $[a, b](a, b) = ab$.

**Problemas**

1. Aplicando el algoritmo euclidiano encontrar el máximo común divisor (m. c. d.) de
   (*a*) 7469 y 2464; (*b*) 2689 y 4001;
   (*c*) 2947 y 3997; (*d*) 1109 y 4999.
2. Encontrar el máximo común divisor $g$ de los números 1819 y 3587 y a continuación encontrar los enteros $x$ y $y$ que satisfagan $1819x + 3587y = g$.
3. Encontrar los valores de $x$ y $y$ que satisfagan
   (*a*) $243x + 198y = 9$;
   (*b*) $71x - 50y = 1$;
   (*c*) $43x + 64y = 1$;
   (*d*) $93x - 81y = 3$;
   (*e*) $6x + 10y + 15z = 1$.
4. Encontrar el mínimo común múltiplo (m.c.m.) de (*a*) 482 y 1687, (*b*) 60 y 61.
5. ¿Cuántos enteros entre 100 y 1000 son divisibles entre 7?
6. Probar que el producto de tres enteros consecutivos es divisible entre 6; de cuatro enteros consecutivos entre 24.
7. Mostrar tres enteros que sean primos relativos pero no primos relativos en pares.
8. Se dice que dos enteros son de la misma paridad si ambos son pares, o bien, ambos son impares: si uno es par y el otro impar, se dice que son de paridad opuesta, o bien, de paridad diferente. Dados dos enteros cualesquiera, probar que su suma y su diferencia son de la misma paridad.
9. Demostrar que si $ac|bc$ entonces $a|b$.
10. Dado $a|b$ y $c|d$, probar que $ac|bd$.

11. Probar que $4 \nmid (n^2 + 2)$ para cualquier entero $n$.
12. Dado que $(a, 4) = 2$ y $(b, 4) = 2$ probar que $(a + b, 4) = 4$.
13. Probar que $n^2 - n$ es divisible entre 2 para todo entero $n$; que $n^3 - n$ es divisible entre 6; que $n^5 - n$ es divisible entre 30.
14. Probar que si $n$ es impar, $n^2 - 1$ es divisible entre 8.
15. Probar que si $x$ y $y$ son impares, entonces $x^2 + y^2$ es par, pero no divisible entre 4.
16. Probar que si $a$ y $b$ son enteros positivos que satisfacen $(a, b) = [a, b]$ entonces $a = b$.
17. Evaluar $(n, n + 1)$ y $[n, n + 1]$ donde $n$ es un entero positivo.
18. Encontrar los valores de $(a, b)$ y $[a, b]$ si $a$ y $b$ son enteros positivos tales que $a|b$.
19. Probar que cualquier conjunto de enteros que sean primos relativos en pares son primos relativos.
20. Dados los enteros $a$ y $b$, se dice que un número $n$ es de la forma $ak + b$ si existe un entero $k$ tal que $ak + b = n$. Así, los números de la forma $3k + 1$ son $\ldots -8, -5, -2, 1, 4, 7, 10, \ldots$. Probar que todo entero es de la forma $3k$, o bien, de la forma $3k + 1$, o bien, de la forma $3k + 2$.
21. Probar que si un entero es de la forma $6k + 5$, entonces es necesariamente de la forma $3k - 1$, pero no inversamente.
22. Probar que el cuadrado de cualquier entero de la forma $5k + 1$ es de la misma forma.
23. Probar que el cuadrado de cualquier entero es de la forma $3k$, o bien, $3k + 1$ pero no de la forma $3k + 2$.
24. Probar que no existen los enteros $x$, $y$ que satisfagan $x + y = 100$ y $(x, y) = 3$.
25. Probar que existen un número infinito de pares de enteros $x$, $y$ que satisfacen $x + y = 100$ y $(x, y) = 5$.
26. Sean dados los enteros $s$ y $g > 0$. Probar que existen los enteros $x$ y $y$ que satisfacen $x + y = s$ y $(x, y) = g$ si, y solamente si $g|s$.
27. Encontrar los enteros positivos $a$ y $b$ que satisfagan simultáneamente las ecuaciones $(a, b) = 10$ y $[a, b] = 100$. Encontrar todas las soluciones.
28. Encontrar todas las tripletas de enteros positivos $a$, $b$, $c$ que satisfagan simultáneamente $(a, b, c) = 10$ y $[a, b, c] = 100$.
29. Sean dados los enteros positivos $g$ y $l$. Probar que existen los enteros $x$ y $y$ que satisfagan $(x, y) = g$ y $[x, y] = l$ si, y solamente si $g|l$.
30. Sean dados los enteros $b$ y $g > 0$. Probar que las ecuaciones $(x, y) = g$ y $xy = b$ pueden resolverse simultáneamente si, y solamente si $g^2|b$.
31. Sean $n \geqq 2$ y $k$ enteros positivos cualesquiera. Probar que $(n - 1)|(n^k - 1)$.
32. Sean $n \geqq 2$ y $k$ enteros positivos cualesquiera. Probar que $(n - 1)^2|(n^k - 1)$ si, y solamente si $(n - 1)|k$. *Sugerencia*: $n^k = \{(n - 1) + 1\}^k$.
33. Probar que $(a, b, c) = ((a, b), c)$.
34. Extender los Teoremas 1.6, 1.7 y 1.8 para los conjuntos de más de dos enteros.
35. Probar que si $(b, c) = 1$ y $r|b$, entonces $(r, c) = 1$.
36. Probar que si $m > n$ entonces $a^{2^n} + 1$ es un divisor de $a^{2^m} - 1$. Demostrar que si $a$, $m$, $n$ son enteros positivos con $m \neq n$, entonces

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1 \text{ si } a \text{ es par,} \\ 2 \text{ si } a \text{ es impar.} \end{cases}$$

## 1.3 Primos

**Definición 1.5** *Se dice que un entero $p>1$ es un número primo, o simplemente que es un primo, en caso de que no exista divisor $d$ de $p$ que satisfaga $1 < d < p$. Si un entero $a > 1$ no es un primo, entonces se dice que es un número compuesto.*

Así, por ejemplo, 2, 3, 5 y 7 son primos, mientras que 4, 6, 8 y 9 son compuestos.

**Teorema 1.14** *Todo entero $n$ mayor que 1 puede expresarse como un producto de primos (con, tal vez, solamente un factor).*

*Demostración.* Si el entero $n$ es primo, entonces el propio entero se presenta como un "producto" con un solo factor. De otra manera, $n$ puede factorizarse en, digamos, $n_1n_2$, donde $1 < n_1 < n$ y $1 < n_2 < n$. Si $n_1$ es primo, se deja; de otra manera se factorizará en $n_3n_4$ donde $1 < n_3 < n_1$ y $1 < n_4 < n_1$; se procede de modo semejante para $n_2$. Este proceso de escribir cada número compuesto que se obtiene como un producto de factores, debe terminar, porque los factores son menores que el propio número compuesto y, no obstante, cada factor es un entero mayor que 1. De donde, podemos escribir $n$ como un producto de primos y, puesto que los factores primos no son necesariamente distintos, el resultado puede escribirse en la forma

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

donde $p_1, p_2, \cdots, p_r$ son primos distintos y $\alpha_1, \alpha_2, \cdots, \alpha_r$ son positivos.

Esta expresión recibe el nombre de representación de $n$ como un producto de primos y salta a la vista que la representación es única en el sentido de que, para un $n$ fijo, cualquiera otra representación simplemente es una permutación de los factores. Puede parecerle obvio al lector que la representación de un entero como un producto de primos es única, pero es un hecho que requiere demostración. En verdad, existen situaciones matemáticas donde podría parecer igualmente "obvio" que la factorización es única pero donde de hecho no lo es. Nos desviaremos de nuestro tema principal para discutir dos de estas situaciones donde la factorización no es única.

Primero, considérese la clase $E$ de los enteros pares positivos, de modo que los elementos de $E$ son 2, 4, 6, 8, 10, . . . . Obsérvese que $E$ es un sistema multiplicativo, el producto de dos elementos cualesquiera de $E$ se encuentra también en $E$. Ahora, limitemos nuestra atención a $E$ en el sentido de que los únicos "números" que conocemos son miembros de

$E$. Entonces $8 = 2 \cdot 4$ es "compuesto", mientras que 10 es "primo" puesto que 10 no es el producto de dos o más "números". Los primos son 2, 6, 10. 14, . . . , los "números compuestos" son 4, 8, 12, . . . . Ahora bien, el "número" 60 tiene dos factorizaciones en "primos", a saber $60 = 2 \cdot 30 = 6 \cdot 10$ y, por tanto, la factorización no es única.

Un ejemplo un poco menos artificial pero también más complicado se obtiene considerando la clase $C$ de números $a + b\sqrt{-6}$ donde $a$ y $b$ recorren todos los enteros. Se dice que este sistema $C$ es cerrado bajo la adición y la multiplicación, dando a entender que la suma y el producto de dos elementos en $C$ son elementos de $C$. Tomando $b = 0$ se observa que los enteros forman un subconjunto de la clase $C$.

Primero estableceremos que existen primos en $C$ y que todo número en $C$ puede factorizarse en primos. Para cualquier número $a + b\sqrt{-6}$ en $C$ será conveniente tener una norma, $N(a + b\sqrt{-6})$, definida como

$$N(a + b\sqrt{-6}) = (a + b\sqrt{-6})(a - b\sqrt{-6}) = a^2 + 6b^2.$$

De donde, la norma de un número en $C$ es el producto del número complejo $a + b\sqrt{-6}$ y su conjugado $a - b\sqrt{-6}$. Otra forma de decirlo, quizá en lenguaje más familiar, es que la norma es el cuadrado del valor absoluto. Ahora bien, la norma de todo número en $C$ es un entero positivo mayor que 1, excepto para los números 0, 1, $-1$ para los cuales se tiene $N(0) = 0$, $N(1) = 1$, $N(-1) = 1$. Se dice que se tiene una factorización de $a + b\sqrt{-6}$ si puede escribirse

$$a + b\sqrt{-6} = (x_1 + y_1\sqrt{-6})(x_2 + y_2\sqrt{-6}), \tag{1.1}$$

donde $N(x_1 + y_1\sqrt{-6}) > 1$ y $N(x_2 + y_2\sqrt{-6}) > 1$. Esta restricción sobre las normas de los factores es necesaria para excluir factorizaciones triviales tales como $a + b\sqrt{-6} = (1)(a + b\sqrt{-6}) = (-1)(-a - b\sqrt{-6})$. La norma de un producto puede calcularse fácilmente como el producto de las normas de los factores, de manera que en la factorización (1.1) se tiene $N(a + b\sqrt{-6}) = N(x_1 + y_1\sqrt{-6})N(x_2 + y_2\sqrt{-6})$. Se deduce que

$$1 < N(x_1 + y_1\sqrt{-6}) < N(a + b\sqrt{-6}),$$
$$1 < N(x_2 + y_2\sqrt{-6}) < N(a + b\sqrt{-6}),$$

y por tanto, cualquier número $a + b\sqrt{-6}$ se descompondrá solamente en un número finito de factores puesto que la norma de cada factor es un entero.

Anteriormente se hizo la observación de que la norma de cualquier número en $C$, aparte de 0 y $\pm 1$, es mayor que 1. Aún puede decirse más. Dado que $N(a + b\sqrt{-6})$ tiene el valor $a^2 + 6b^2$, se observa que

(1.2) $$N(a + b\sqrt{-6}) \geqq 6 \quad \text{si} \quad b \neq 0,$$

esto es, la norma de cualquier número complejo en $C$ no es menor que 6.

Un número de $C$ que tiene norma $> 1$, pero el cual no puede factorizarse en la forma establecida en (1.1), es un primo en $C$. Por ejemplo 5 es un primo en $C$. Porque, en primer lugar, 5 no puede factorizarse en números reales en $C$. En segundo lugar, si se tuviera una factorización $5 = (x_1 + y_1\sqrt{-6})(x_2 + y_2\sqrt{-6})$ en números complejos, podríamos tomar las normas para obtener

$$25 = N(x_1 + y_1\sqrt{-6})N(x_2 + y_2\sqrt{-6}),$$

lo cual contradice (1.2). Por tanto, 5 es un primo en $C$, y un argumento semejante establece que 2 es un primo.

Ahora estamos en posición de demostrar que no todos los números de $C$ se factorizan unívocamente en primos. Considérese el número 10 y sus dos factorizaciones

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

El primer producto $2 \cdot 5$ tiene factores que son primos en $C$, tal y como se vio anteriormente. Así que, puede concluirse que no existe factorización única del número 10 en $C$. Nótese que esta conclusión no depende de nuestro conocimiento de que $2 + \sqrt{-6}$ y $2 - \sqrt{-6}$ son primos; realmente lo son pero no tiene importancia para nuestra discusión.

Regresemos ahora a la discusión de la factorización única en los enteros ordinarios $0, \pm 1, \pm 2, \cdots$. Será conveniente tener el siguiente resultado.

**Teorema 1.15** *Si $p|ab$, $p$ siendo primo, entonces $p|a$ o bien $p|b$. Más generalmente, si $p|a_1a_2 \cdots a_n$, entonces $p$ divide por lo menos a un factor $a_i$ del producto.*

*Demostración.* Si $p \nmid a$, entonces $(a, p) = 1$ y así, por el Teorema 1.10, $p|b$. Puede considerarse esto como el primer paso de una demostración por inducción matemática de la proposición general. Por tanto, supóngase que la proposición se cumple siempre que $p$ divide a un producto con menos de $n$ factores. Ahora bien, si $p|a_1a_2 \cdots a_n$, esto es, $p|a_1c$ donde $c = a_2a_3 \cdots a_n$, entonces $p|a_1$ o bien $p|c$. Si $p|c$ se aplica la hipótesis de inducción para concluir que $p|a_i$ para algún subíndice $i$.

**Teorema 1.16** *El teorema fundamental de la aritmética. La factorización de cualquier entero positivo $n$ en primos es única independientemente del orden de los primos.*

*Primera demostración.* Supóngase que existe un entero $n$ con dos factorizaciones diferentes. Dividiendo entre los primos comunes a las dos representaciones, se tendría una igualdad de la forma

$$p_1p_2 \cdots p_r = q_1q_2 \cdots q_s \tag{1.3}$$

donde los factores $p_i$ y $q_j$ son primos, no necesariamente todos distintos, pero donde ningún primo del primer miembro se tiene en el segundo miembro. Pero esto es imposible $p_1|q_1q_2 \cdots q_s$, y así, por el Teorema 1.15, $p_1$ es un divisor de por lo menos uno de los $q_j$. Es decir, $p_1$ debe ser idéntico a por lo menos uno de los $q_j$.

*Segunda demostración.* Supóngase que el teorema es falso y sea $n$ el menor entero positivo que tiene más de una representación como el producto de primos, digamos

$$n = p_1p_2 \cdots p_r = q_1q_2 \cdots q_s. \tag{1.4}$$

Es evidente que $r$ y $s$ son mayores que 1. Ahora bien, los primos $p_1$, $p_2$, $\ldots, p_r$ no tienen miembros en común con $q_1$, $q_2$, $\ldots, q_s$ porque si, por ejemplo, $p_1$ fuera un primo común, entonces podría dividirse ambos miembros de (1.4) para obtener dos factorizaciones distintas de $n/p_1$. Pero esto contradiría la suposición de que todos los enteros menores que $n$ son factorizables unívocamente.

A continuación, no existe pérdida de generalidad al suponer que $p_1 < q_1$ y definir el entero positivo $N$ como

$$N = (q_1 - p_1)q_2q_3 \cdots q_s = p_1(p_2p_3 \cdots p_r - q_2q_3 \cdots q_s). \tag{1:5}$$

Es evidente que $N < n$, de manera que $N$ es unívocamente factorizable en primos. Pero $p_1 \nmid (q_1 - p_1)$, así que (1.5) proporciona dos factorizaciones de $N$, una conteniendo a $p_1$ y la otra no, y así se llega a una contradicción.

Puede observarse que la segunda demostración del Teorema 1.16 no depende del Teorema 1.15, ni siquiera de cualquier otro teorema anterior. Por tanto, sería posible poner el Teorema 1.16 más cerca del principio del estudio de la teoría de los números y deducir como consecuencias tales resultados como los Teoremas 1.8, 1.10 y 1.15. Sin embargo, no todos los resultados anteriores son consecuencias del teorema fundamental.

En la aplicación del teorema fundamental frecuentemente se escribe cualquier entero $a > 1$ en la forma

$$a = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

en ocasiones llamada "forma canónica", donde los primos $p_i$ son distintos y los exponentes $\alpha_i$ son positivos. Sin embargo, algunas veces es conveniente usar una ligera variación de la forma canónica y permitir

que algunos exponentes sean cero. Por ejemplo, si se desea describir el máximo común divisor $g$ de $a$ y $b$ en términos de los factores primos de $a$ y $b$, podría escribirse

$$(1.6) \qquad a = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \qquad b = p_1^{\beta_1}p_2^{\beta_2} \cdots p_r^{\beta_r}$$

donde $\alpha_i \geqq 0$ y $\beta_i \geqq 0$. Entonces se ve que el máximo común divisor es

$$g = (a, b) = p_1^{\text{mín}\,(\alpha_1,\beta_1)}\, p_2^{\text{mín}\,(\alpha_2,\beta_2)} \cdots p_r^{\text{mín}\,(\alpha_r,\beta_r)}$$

donde mín$(\alpha, \beta)$ denota el mínimo de $\alpha$ y $\beta$. En el caso de que $a = 108$ y $b = 225$, se tendría

$$a = 2^2 3^3 5^0, \quad b = 2^0 3^2 5^2, \quad g = 2^0 3^2 5^0 = 9.$$

De modo semejante, se ve que el mínimo común múltiplo de $a$ y $b$ es

$$[a, b] = p_1^{\text{máx}\,(\alpha_1,\beta_1)}\, p_2^{\text{máx}\,(\alpha_2,\beta_2)} \cdots p_r^{\text{máx}\,(\alpha_r,\beta_r)}$$

donde máx $(\alpha, \beta)$ denota el máximo de $\alpha$ y $\beta$. Si ningún $\alpha_i$ es mayor que 1, se dice que $a$ es exento de cuadrados.

**Teorema 1.17** *Euclides. El número de primos es infinito. Esto es, no existe fin para la sucesión de primos*

$$2, 3, 5, 7, 11, 13, \ldots .$$

*Demostración.* Supóngase que existiera solamente un número finito de primos $p_1, p_2, \ldots, p_r$. Entonces fórmese el número

$$n = 1 + p_1 p_2 \cdots p_r.$$

Nótese que $n$ no es divisible entre $p_1$, o bien $p_2$ o bien $\ldots$ $p_r$. De aquí que cualquier divisor primo $p$ de $n$ es un primo distinto de $p_1, p_2, \ldots, p_r$. Puesto que $n$ es primo o bien tiene un factor primo $p$, esto implica que existe un primo distinto de $p_1, p_2, \ldots, p_r$.

**Teorema 1.18** *Existen arbitrariamente grandes vacíos en la serie de los primos. Dicho de otra manera, dado cualquier entero positivo $k$, existen $k$ enteros compuestos consecutivos.*

*Demostración.* Considérense los enteros

$$(k + 1)! + 2, (k + 1)! + 3, \ldots, (k + 1)! + k, (k + 1)! + k + 1.$$

Cada uno de éstos es compuesto porque $j$ divide a $(k + 1)! + j$ si $2 \leqq j \leqq k + 1$.

Los primos están espaciados irregularmente, tal y como la sugiere el último teorema. Si se denota el número de primos que no exceden a $x$ por $\pi(x)$, podría preguntarse acerca de la naturaleza de esta función. Debido a lo irregular de la ocurrencia de los primos, no puede esperarse

una fórmula sencilla para $\pi(x)$. Sin embargo, uno de los resultados más impresionantes de la teoría avanzada de los números, el teorema de los números primos, proporciona una aproximación asintótica para $\pi(x)$. Establece que

$$\lim_{x\to\infty} \pi(x)\,\frac{\log x}{x} = 1,$$

es decir, que la razón de $\pi(x)$ a $x/\log x$ tiende hacia 1 conforme $x$ se hace indefinidamente grande.

**Problemas**

1. En cualquier entero positivo, tal como 8347, el último dígito se llama dígito de las unidades, el siguiente, dígito de las decenas, el siguiente, dígito de las centenas, etc. En el ejemplo 8347, el dígito de las unidades es 7, el dígito de las decenas es 4, el dígito de las centenas es 3 y el dígito de los millares es 8. Probar que el número es divisible entre 2 si, y solamente si el dígito de las unidades es divisible entre 2; que el número es divisible entre 4, si, y solamente si el entero formado por su dígito de las decenas y su dígito de las unidades es divisible entre 4; que el número es divisible entre 8, si, y solamente si el entero formado por sus tres últimos dígitos es divisible entre 8.
2. Probar que cualquier entero es divisible entre 3 si, y solamente si la suma de sus dígitos es divisible entre 3. Probar que cualquier entero es divisible entre 9 si, y solamente si la suma de sus dígitos es divisible entre 9.
3. Probar que cualquier entero es divisible entre 11 si, y solamente si la diferencia entre la suma de los dígitos que se encuentran en los lugares impares y la suma de los dígitos que se encuentran en los lugares pares es divisible entre 11.
4. Demostrar que todo entero positivo $n$ tiene una expresión única de la forma $n = 2^r m$, $r \geqq 0$, $m$ un entero positivo impar.
5. Sean $a/b$ y $c/d$ fracciones en su más simple expresión, de manera que $(a, b) = (c, d) = 1$. Probar que si su suma es un entero, entonces $|b| = |d|$.
6. Probar que si un número racional $r/s$ en su más simple expresión satisface una ecuación $x^m = a$, donde $a$ es un entero, entonces $s = \pm 1$. De donde, las únicas soluciones racionales, si existen, de $x^m = a$ son enteros.
7. Usar el problema precedente para probar que $x^2 = 2$, $x^3 = 3$ y $x^4 = 7$ no tienen soluciones racionales. Así que $\sqrt{2}$, $\sqrt[3]{3}$, $\sqrt[4]{7}$ son irracionales. En general, probar que $x^m = a$ no tiene soluciones racionales a menos que $a$ sea la $m$-ésima potencia de un entero.
8. Probar que cualquier primo de la forma $3k + 1$ es de la forma $6k + 1$.
9. Probar que cualquier entero positivo de la forma $3k + 2$ tiene un factor primo de la misma forma; de modo semejante, para cada una de las formas $4k + 3$ y $6k + 5$.
10. Si $x$ y $y$ son impares, probar que $x^2 + y^2$ no puede ser un cuadrado perfecto.
11. Si $x$ y $y$ son primos para 3, probar que $x^2 + y^2$ no puede ser un cuadrado perfecto.

12. Probar que $(a, b) = (a, b, a + b)$ y, más generalmente, que $(a, b) = (a, b, ax + by)$ para todos los enteros $x$, $y$.
13. Probar que $(a, a + k)|k$ para todos los enteros $a$, $k$ no ambos cero.
14. Probar que $(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n)$.
15. Probar que $(a, a + 2) = 1$, o bien, 2 para todo entero $a$.
16. Si $(a, b) = p$, un primo, ¿cuáles son los valores posibles de $(a^2, b)$? ¿De $(a^3, b)$? ¿De $(a^2, b^3)$?
17. Evaluar $(ab, p^4)$ y $(a + b, p^4)$ dado que $(a, p^2) = p$ y $(b, p^3) = p^2$ donde $p$ es un primo.
18. Si $a$ y $b$ se representan por (1.6), ¿qué condiciones deben satisfacer los exponentes si $a$ debe ser un cuadrado perfecto? ¿Un cubo perfecto? (Para que $a|b$? ¿Para que $a^2|b^2$?
19. Probar la segunda parte del Teorema 1.13 mediante el uso de las fórmulas para el m. c. d. y m. c. m. obtenidas de (1.6).
20. Probar que $(a^2, b^2) = c^2$ si $(a, b) = c$.
21. Sean $a$ y $b$ enteros positivos tales que $(a, b) = 1$ y $ab$ es un cuadrado perfecto. Probar que $a$ y $b$ son cuadrados perfectos. Probar que el resultado se generaliza para las $k$-ésimas potencias.
22. Dado $(a, b, c)\,[a, b, c] = abc$, probar que $(a, b) = (b, c) = (a, c) = 1$.
23. Probar que $[a, b, c]\,(ab, bc, ca) = |abc|$.
24. Determinar si las siguientes aseveraciones son verdaderas o falsas. Si son verdaderas, probar el resultado, y si son falsas, dar un contraejemplo.
    (1) Si $(a, b) = (a, c)$, entonces $[a, b] = [a, c]$.
    (2) Si $(a, b) = (a, c)$, entonces $(a^2, b^2) = (a^2, c^2)$.
    (3) Si $(a, b) = (a, c)$, entonces $(a, b) = (a, b, c)$.
    (4) Si $p$ es un primo y $p|a$ y $p|(a^2 + b^2)$, entonces $p|b$.
    (5) Si $p$ es un primo y $p|a^7$, entonces $p|a$.
    (6) Si $a^3|c^3$, entonces $a|c$.
    (7) Si $a^3|c^2$, entonces $a|c$.
    (8) Si $a^2|c^3$, entonces $a|c$.
    (9) Si $p$ es un primo y $p|(a^2 + b^2)$ y $p|(b^2 + c^2)$, entonces $p|(a^2 - c^2)$.
    (10) Si $p$ es un primo y $p|(a^2 + b^2)$ y $p|(b^2 + c^2)$, entonces $p|(a^2 + c^2)$.
    (11) Si $(a, b) = 1$, entonces $(a^2, ab, b^2) = 1$.
    (12) $[a^2, ab, b^2] = [a^2, b^2]$.
    (13) Si $b|(a^2 + 1)$, entonces $b|(a^4 + 1)$.
    (14) Si $b|(a^2 - 1)$, entonces $b|(a^4 - 1)$.
    (15) $(a, b, c) = ((a, b), (a, c))$.
25. ¿Para cuáles enteros positivos $n$ es cierto que

$$\sum_{j=1}^{n} j \,\Big|\, \prod_{j=1}^{n} j?$$

26. Dados los enteros positivos $a$ y $b$ tales que $a|b^2$, $b^2|a^3$, $a^3|b^4$, $b^4|a^5$, . . . , probar que $a = b$.
27. Dados los enteros $a$, $b$, $c$, $d$, $m$, $n$, $u$, $v$ que satisfacen $ad - bc = \pm 1$, $u = am + bn$, $v = cm + dn$, probar que $(m, n) = (u, v)$.
28. Probar que si $n$ es compuesto tiene un divisor primo $p$ que satisface $p \leqq \sqrt{n}$.
29. Obtener una lista completa de los primos entre 1 y $n$, con $n = 200$ por conveniencia, mediante el método siguiente, conocido como la "criba de Eratóstenes". Por múltiplos "propios" de $k$ se entiende todos los múltiplos

positivos de $k$ excepto el propio $k$. Escribir todos los números desde 2 hasta 200. Tachar todos los múltiplos propios de 2, a continuación los de 3, a continuación los de 5. En cada paso, el siguiente número mayor restante es primo. Así que, 7 es ahora el siguiente número restante mayor que 5. Tachar los múltiplos propios de 7. El siguiente número restante mayor que 7 es 11. A continuación, se tachan los múltiplos propios de 11 y después los de 13. Ahora, obsérvese que el siguiente número restante mayor que 13 excede a $\sqrt{200}$ y de aquí que, de acuerdo con el problema anterior, todos los números restantes en la lista son primos.

30. Considérese el conjunto $S$ de enteros $1, 2, 3, \ldots, n$. Sea $2^k$ el entero en $S$ el cual es la mayor potencia de 2. Probar que $2^k$ no es un divisor de cualquier otro entero en $S$.
31. Probar que $\sum_{j=1}^{n} 1/j$ no es un entero si $n > 1$.
32. Considérese el conjunto $T$ de enteros $1, 3, 5, \cdots, 2n - 1$. Sea $3^r$ el entero en $T$ el cual es la mayor potencia de 3. Probar que $3^r$ no es un divisor de cualquier otro entero de $T$.
33. Probar que $\sum_{j=1}^{n} 1/(2j - 1)$ no es un entero si $n > 1$.
34. Se dice que un entero positivo $n$ es una suma de enteros consecutivos si existen los enteros positivos $m$ y $k$ de manera que $n = m + (m + 1) + \cdots + (m + k)$. Probar que $n$ es expresable así, si y solamente si no es una potencia de 2.
35. Si $2^n + 1$ es un primo impar, probar que $n$ es una potencia de 2.
36. Si $2^n - 1$ es un primo, probar que $n$ es primo.
37. Si $a$ y $b > 2$ son enteros positivos cualesquiera, probar que $2^a + 1$ no es divisible entre $2^b - 1$.
38. Sean dados los enteros positivos $g$ y $l$ con $g|l$. Probar que el número de pares de enteros positivos $x, y$ que satisfacen $(x, y) = g$ y $[x, y] = l$ es $2^k$, donde $k$ es el número de factores primos distintos de $l/g$. (Considerar $x_1, y_1$ y $x_2, y_2$ como pares diferentes si $x_1 \neq x_2$, o bien $y_1 \neq y_2$).
39. Sea $k \geqq 3$ un entero fijo. Encontrar todos los conjuntos $a_1, a_2, \ldots, a_k$ de enteros positivos, tales que, la suma de cualquier tripleta sea divisible entre cada miembro de la tripleta.
40. Probar que $2 + \sqrt{-6}$ y $2 - \sqrt{-6}$ son primos en la clase $C$ de números $a + b\sqrt{-6}$.
41. Probar el Teorema 1.13 mediante la aplicación del teorema fundamental.
42. Probar que todo entero positivo es expresable unívocamente en la forma

$$2^{j_0} + 2^{j_1} + 2^{j_2} + \cdots + 2^{j_m}$$

donde $m \geqq 0$ y $0 \leqq j_0 < j_1 < j_2 < \cdots < j_m$.

43. Probar que cualquier entero positivo $a$ puede expresarse unívocamente en la forma

$$a = 3^m + b_{m-1}3^{m-1} + b_{m-2}3^{m-2} + \cdots + b_0,$$

donde cada $b_j = 0, 1$, o bien, $-1$.

44. Probar que no existen enteros positivos $a, b, n > 1$, tales que $(a^n - b^n) | (a^n + b^n)$.
45. Probar que ningún polinomio $f(x)$ con coeficientes enteros puede representar un primo para todo entero positivo $x$. *Sugerencia*: si $f(j) = p$ enton-

ces $f(j + kp) - f(j)$ es un múltiplo de $p$ para todo $k$ y así $f(j + kp)$ tiene la misma propiedad.

46. Probar que existe un número infinito de primos considerando la sucesión $2^{2^1} + 1$, $2^{2^2} + 1$, $2^{2^3} + 1$, $2^{2^4} + 1, \ldots$ . *Sugerencia*: aplicar el resultado del problema 36 de la sección 1.2.

47. Probar que existe un número infinito de primos de la forma $4n + 3$; de la forma $6n + 5$.

*Observación*. El último problema puede establecerse del modo siguiente: cada una de las progresiones aritméticas 3, 7, 11, 15, 19, . . . y 5, 11, 17, 23, 29, . . . contiene una infinidad de primos. Uno de los teoremas famosos de la teoría de los números (la demostración del cual se encuentra más allá de los métodos de este libro), debido a Dirichlet, es que la progresión aritmética $a, a + b, a + 2b, a + 3b, \ldots$ contiene un número infinito de primos si los enteros $a$ y $b > 0$ son primos relativamente, esto es si $(a, b) = 1$.

# Capítulo 2

# Congruencias

## 2.1 Congruencias

Salta a la vista, con bases en lo tratado en el capítulo 1, que la divisibilidad es un concepto fundamental de la teoría de los números, uno que la coloca aparte de muchas otras ramas de las matemáticas. En este capítulo continuaremos el estudio de la divisibilidad, pero desde un punto de vista ligeramente diferente. Una congruencia no es otra cosa que una afirmación acerca de la divisibilidad. Sin embargo es más que una notación conveniente. Con frecuencia facilita el descubrimiento de las demostraciones, y se verá que las congruencias pueden sugerir nuevos problemas que nos conducirán hacia tópicos nuevos e interesantes.

**Definición 2.1** *Si un entero $m$, diferente de cero, divide a la diferencia $a - b$, se dice que $a$ es congruente con $b$ módulo $m$ y se escribe $a \equiv b \pmod{m}$. Si $a - b$ no es divisible entre $m$, se dice que $a$ no es congruente con $b$ módulo $m$ y en este caso se escribe $a \not\equiv b \pmod{m}$.*

Puesto que $a - b$ es divisible entre $m$ si y solamente si $a - b$ es divisible entre $-m$, por lo general restringiremos nuestra atención a los módulos positivos. De hecho, en todo el presente capítulo se supondrá que el módulo $m$ es un entero positivo.

Las congruencias tienen muchas propiedades en común con las igualdades. Algunas de las propiedades que se deducen fácilmente a partir de la definición se enlistan en el siguiente teorema.

**Teorema 2.1** *Supóngase que $a, b, c, d, x, y$, denotan enteros. Entonces:*

*a*) $a \equiv b \pmod{m}$, $b \equiv a \pmod{m}$ y $a - b \equiv 0 \pmod{m}$ *son proposiciones equivalentes.*
*b*) *Si* $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, *entonces* $a \equiv c \pmod{m}$.
*c*) *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces* $ax + cy \equiv bx + dy \pmod{m}$.
*d*) *Si* $a \equiv b \pmod{m}$ *y* $c \equiv d \pmod{m}$, *entonces* $ac \equiv bd \pmod{m}$.
*e*) *Si* $a \equiv b \pmod{m}$ *y* $d|m$, $d > 0$, *entonces* $a \equiv b \pmod{d}$.

**Teorema 2.2** *Supóngase que f denota un polinomio con coeficientes enteros. Si* $a \equiv b \pmod{m}$ *entonces* $f(a) \equiv f(b) \pmod{m}$.

*Demostración.* Puede suponerse que $f(x) = c_0x^n + c_1x^{n-1} + \cdots + c_n$ donde los $c_i$ son enteros. Supuesto que $a \equiv b \pmod{m}$, puede aplicarse repetidamente el Teorema 2.1*d* para encontrar $a^2 \equiv b^2$, $a^3 \equiv b^3$, $\ldots, a^n \equiv b^n \pmod{m}$, por lo tanto $c_ja^{n-j} \equiv c_jb^{n-j} \pmod{m}$ y, finalmente, $c_0a^n + c_1a^{n-1} + \cdots + c_n \equiv c_0b^n + c_1b^{n-1} + \cdots + c_n \pmod{m}$, por el Teorema 2.1*c*.

Por supuesto que el lector está bien enterado de la propiedad de los números reales que si $ax = ay$ y $a \neq 0$, entonces $x = y$. Debe tenerse más cuidado al dividir una congruencia entre $a$.

**Teorema 2.3**

*a*) $ax \equiv ay \pmod{m}$ *si y solamente si* $x \equiv y \left(\bmod \dfrac{m}{(a, m)}\right)$
*b*) *Si* $ax \equiv ay \pmod{m}$ *y* $(a, m) = 1$, *entonces* $x \equiv y \pmod{m}$.
*c*) $x \equiv y \pmod{m_i}$ *para* $i = 1, 2, \ldots, r$ *si y solamente si* $x \equiv y \pmod{[m_1, m_2, \ldots, m_r]}$.

*Demostración. a*) Si $ax \equiv ay \pmod{m}$ entonces $ay - ax = mz$ para algún entero $z$. De aquí que se tiene

$$\frac{a}{(a, m)}(y - x) = \frac{m}{(a, m)}z$$

y por tanto

$$\frac{m}{(a, m)} \Bigg| \frac{a}{(a, m)}(y - x).$$

Pero $(a/(a, m), m/(a, m)) = 1$, por el Teorema 1.7 y por tanto $\{m/(a, m)\}|(y - x)$ por el Teorema 1.10. Esto implica que

$$x \equiv y \pmod{m/(a, m)}.$$

Si $x \equiv y \pmod{m/(a, m)}$ entonces $\{m/(a, m)\}|(y - x)$ y de aquí que $m|(a, m)(y - x)$. Usando el Teorema 1.1 se obtiene $m|a(y - x)$ y, en consecuencia, se concluye que $ax \equiv ay \pmod{m}$.

*b*) Este es un caso especial de la parte (*a*). Se enlista por separado porque se usará con mucha frecuencia.

*c*) Si $x \equiv y \pmod{m_i}$ para $i = 1, 2, \cdots, r$, entonces $m_i | (y - x)$ para $i = 1, 2, \cdots, r$. Esto es, $y - x$ es un múltiplo común de $m_1, m_2, \cdots, m_r$ y, por tanto, (ver Teorema 1.12) $[m_1, m_2, \cdots, m_r] | (y - x)$. Esto implica que $x \equiv y \pmod{[m_1, m_2, \cdots, m_r]}$.

Si $x \equiv y \pmod{[m_1, m_2, \cdots, m_r]}$ entonces $x \equiv y \pmod{m_i}$ por el Teorema 2.1*e*, puesto que $m_i | [m_1, m_2, \cdots, m_r]$.

Al trabajar con los enteros módulo $m$ esencialmente se realizan las operaciones ordinarias de la aritmética pero pasando por alto los múltiplos de $m$. Bajo un aspecto no se distingue entre $a$ y $a + mx$, donde $x$ es un entero cualquiera. Dado cualquier entero $a$, sean $q$ y $r$ el cociente y el residuo en la división entre $m$; por tanto, por el Teorema 1.2, $a = qm + r$. Ahora $a \equiv r \pmod{m}$ y, dado que $r$ satisface las desigualdades $0 \leqq r < m$, se ve que todo entero es congruente módulo $m$ para uno de los valores $0, 1, 2, \cdots, m - 1$. También es evidente que no existen dos de estos enteros $m$ que sean congruentes módulo $m$. Estos valores $m$ constituyen un sistema completo de residuos módulo $m$ y a continuación se dará una definición general de este término.

**Definición 2.2** *Si $x \equiv y \pmod{m}$ entonces $y$ recibe el nombre de residuo de $x$ módulo $m$. Un conjunto $x_1, x_2, \cdots, x_m$ es un sistema completo de residuos módulo $m$ si para todo entero $y$ existe uno y solamente un $x_j$ tal que $y \equiv x_j \pmod{m}$.*

Es obvio que existe un número infinito de sistemas completos de residuos módulo $m$, siendo otro ejemplo el conjunto $1, 2, \cdots, m - 1$.

Un conjunto de enteros forma un sistema completo de residuos módulo $m$ si y solamente si no se tienen dos enteros en el conjunto que sean congruentes módulo $m$.

**Teorema 2.4** *Si $x \equiv y \pmod{m}$ entonces $(x, m) = (y, m)$.*

*Demostración.* Se tiene $y - x = mz$ para algún entero $z$. Puesto que $(x, m) | x$ y $(x, m) | m$, se tiene $(x, m) | y$ y de aquí que $(x, m) | (y, m)$. En la misma forma se encuentra que $(y, m) | (x, m)$ y entonces se tiene $(x, m) = (y, m)$ por el Teorema 1.1, dado que $(x, m)$ y $(y, m)$ son positivos.

**Definición 2.3** *Un sistema reducido de residuos módulo $m$ es un conjunto de enteros $r_i$ tales que $(r_i, m) = 1$, $r_i \not\equiv r_j \pmod{m}$ si $i \neq j$ y tales que todo $x$ primo para $m$ es congruente módulo $m$ para algún miembro $r_i$ del conjunto.*

En virtud del Teorema 2.4, es evidente que un sistema reducido de residuos módulo $m$ puede obtenerse eliminando aquellos miembros que no son primos relativos para $m$ en el sistema completo de residuos módulo $m$. Además, todos los sistemas de residuos módulo $m$ contendrán el mismo número de miembros, un número que se denota por $\phi(m)$. Esta función recibe el nombre de función $\phi$ de Euler, en ocasiones llamada el totient. Aplicando esta definición de $\phi(m)$ al sistema completo de residuos $1, 2, \cdots, m$ mencionado en el párrafo siguiente a la Definición 2.2, puede obtenerse lo que equivale a otra definición de $\phi(m)$, tal y como se da en el teorema siguiente.

**Teorema 2.5** *El número $\phi(m)$ es el número de enteros positivos menores que o iguales a m son relativamente primos para m.*

**Teorema 2.6** *Sea $(a, m) = 1$. Sea $r_1, r_2, \cdots, r_n$ un sistema completo, o bien, reducido, de residuos módulo m. Entonces $ar_1, ar_2, \cdots, ar_n$ es un sistema completo, o bien, reducido, respectivamente, de residuos módulo m.*

*Demostración.* Si $(r_i, m) = 1$ entonces $(ar_i, m) = 1$, por el Teorema 1.8.

Se tiene el mismo número de $ar_1, ar_2, \cdots, ar_n$ que de $r_1, r_2, \cdots, r_n$. Por lo tanto, solamente es necesario demostrar que $ar_i \not\equiv ar_j \pmod{m}$ si $i \neq j$. Pero el Teorema 2.3*b* establece que $ar_i \equiv ar_j \pmod{m}$ implica $r_i \equiv r_j \pmod{m}$ y de aquí que $i = j$.

**Teorema 2.7** *Teorema de Fermat. Considérese que p denota un primo. Si $p \nmid a$ entonces $a^{p-1} \equiv 1 \pmod{p}$. Para todo entero a, $a^p \equiv a \pmod{p}$.*

Aplazaremos la demostración de este teorema y la obtendremos como un corolario del Teorema 2.8.

**Teorema 2.8** *Generalización de Euler del teorema de Fermat. Si $(a, m) = 1$ entonces*

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

*Demostración.* Sea $r_1, r_2, \cdots, r_{\phi(m)}$ un sistema reducido de residuos módulo $m$. Entonces, por el Teorema 2.6, $ar_1, ar_2, \cdots, ar_{\phi(m)}$ también es un sistema reducido de residuos módulo $m$. De aquí que correspondiendo a cada $r_i$ existe uno y solamente un $ar_j$ tal que $r_i \equiv ar_j \pmod{m}$. Además, diferentes $r_i$ tendrán diferentes $ar_j$ correspondientes. Esto significa que los números $ar_1, ar_2, \cdots, ar_{\phi(m)}$ son precisamente los residuos módulo $m$ de $r_1, r_2, \cdots, r_{\phi(m)}$ pero no necesariamente en el mismo orden. Multiplicando y aplicando el Teorema 2.1*d* se obtiene

$$\prod_{j=1}^{\phi(m)} (ar_j) \equiv \prod_{i=1}^{\phi(m)} r_i \pmod{m}$$

y de aquí que

$$a^{\phi(m)} \prod_{j=1}^{\phi(m)} r_j \equiv \prod_{j=1}^{\phi(m)} r_j \pmod{m}.$$

Ahora bien, $(r_j, m) = 1$ por tanto puede aplicarse el Teorema 2.3*b* para cancelar los $r_j$ y obtener $a^{\phi(m)} \equiv 1 \pmod{m}$.

**Corolario.** *Demostración del Teorema* 2.7. Si $p \nmid a$ entonces $(a, p) = 1$ y $a^{\phi(p)} \equiv 1 \pmod{p}$. Para encontrar $\phi(p)$ nos referimos al Teorema 2.5. Todos los enteros $1, 2, \ldots, p-1, p$ con la excepción de $p$ son relativamente primos para $p$. Así que se tiene $\phi(p) = p - 1$ y se concluye la primera parte del teorema de Fermat. La segunda parte es ahora obvia.

**Corolario 2.9** *Si* $(a, m) = 1$ *entonces* $ax \equiv b \pmod{m}$ *tiene una solución* $x = x_1$. *Todas las soluciones están dadas por* $x = x_1 + jm$ *donde* $j = 0, \pm 1, \pm 2, \cdots$.

*Demostración.* Supuesto que $(1, m) = 1$ y $1 \leqq m$, se ve que $\phi(m) \geqq 1$. Entonces simplemente es necesario hacer $x_1 = a^{\phi(m)-1}b$.

Si $x$ es cualquier solución entonces $ax - ax_1 \equiv b - b \equiv 0 \pmod{m}$ y de aquí que $a(x - x_1) \equiv 0 \pmod{m}$. Usando el Teorema 2.3*b* se obtiene $x - x_1 \equiv 0 \pmod{m}$ lo cual implica que $x = x_1 + jm$. El hecho de que todos son realmente soluciones se deduce del Teorema 2.2.

La función $\phi(m)$ de Euler es sumamente interesante. La consideraremos posteriormente en las secciones 2.4 y 4.2.

**Teorema 2.10** *Teorema de Wilson. Si* $p$ *es un primo, entonces* $(p-1)! \equiv -1 \pmod{p}$.

*Demostración.* Si $p = 2$ o bien $p = 3$ la congruencia se verifica fácilmente.

Ahora puede suponerse $p \geqq 5$. La idea fundamental de la demostración es muy sencilla pero debe tenerse un poco de cuidado. Considérense los enteros cuyo producto es $(p-1)!$ y trátese de parearlos en tal forma que el producto de los dos miembros de cada par sea congruente a 1 módulo $p$.

Dado un entero $j$ que satisfaga $1 \leqq j \leqq p - 1$, entonces $(j, p) = 1$ y se ve, por el Corolario 2.9, que existe exactamente un entero $i$ tal que $ji \equiv 1 \pmod{p}$ y $0 \leqq i \leqq p - 1$. Obviamente $i = 0$ es imposible, de

modo que se tiene $1 \leqq i \leqq p - 1$. Asóciese a cada $j$ el correspondiente entero $i$. Dado que $ij \equiv ji \equiv 1 \pmod{p}$ se ve que $j$ es el entero asociado con $i$. El entero 1 se asocia consigo mismo, al igual que $p - 1$. Omitiendo por un momento estos valores considérese $2 \leqq j \leqq p - 2$. Para estos $j$ se tiene $(j-1, p) = (j+1, p) = 1$, de donde $j^2 - 1 = (j-1)(j+1) \not\equiv 0 \pmod{p}$, por el Teorema 1.8. Por lo tanto, cada uno de estos $j$ se asocia con un $i \neq j$, $2 \leqq i \leqq p - 2$ y el asociado de $i$ es el propio $j$. Así que los enteros $2, 3, \ldots, p - 2$ pueden parearse, $j$ y su asociado $i$, y $ji \equiv 1 \pmod{p}$. Multiplicando todos estos pares juntos se obtiene $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p}$ y se llega a la conclusión del teorema de Wilson porque $1 \cdot (p-1) \equiv -1 \pmod{p}$.

Los teoremas de Wilson y de Fermat pueden aplicarse para determinar aquellos primos $p$ para los cuales $x^2 \equiv -1 \pmod{p}$ tiene una solución. Esto es un caso especial de algunos resultados que se estudiarán posteriormente (ver capítulo 3). Sin embargo, es interesante ver que este caso especial puede manejarse mediante procedimientos relativamente sencillos.

**Teorema 2.11** *Sea $p$ un primo. Entonces $x^2 \equiv -1 \pmod{p}$ tiene soluciones si y solamente si $p = 2$ o bien $p \equiv 1 \pmod{4}$.*

*Demostración.* Si $p = 2$ se tiene la solución $x = 1$.

Para cualquier primo impar $p$ puede escribirse el teorema de Wilson en la forma

$$\left(1 \cdot 2 \cdots j \cdots \frac{p-1}{2}\right)\left(\frac{p+1}{2} \cdots (p-j) \cdots (p-2)(p-1)\right) \equiv -1 \pmod{p}.$$

El producto del primer miembro se ha dividido en dos partes, cada una con el mismo número de factores. Pareando los $j$ de la primera mitad con los $p - j$ de la segunda mitad, puede reescribirse la congruencia en la forma

$$\prod_{j=1}^{(p-1)/2} j(p-j) \equiv -1 \pmod{p}.$$

Pero $j(p-j) \equiv -j^2 \pmod{p}$ y así se tiene, si $p \equiv 1 \pmod{4}$,

$$\prod_{j=1}^{(p-1)/2} j(p-j) \equiv \prod_{j=1}^{(p-1)/2} (-j^2) \equiv (-1)^{(p-1)/2}\left(\prod_{j=1}^{(p-1)/2} j\right)^2 \equiv \left(\prod_{j=1}^{(p-1)/2} j\right)^2 \pmod{p}$$

y de donde se tiene una solución $\prod_{j=1}^{(p-1)/2} j$, de $x^2 \equiv -1 \pmod{p}$.

Si $p \neq 2$ y $p \not\equiv 1 \pmod 4$, entonces $p \equiv 3 \pmod 4$. En este caso, si para algún entero $x$, $x^2 \equiv -1 \pmod p$, entonces se tiene $x^{p-1} \equiv (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv -1 \pmod p$, dado que $(p-1)/2 \equiv 1 \pmod 2$. Pero evidentemente $p \nmid x$ y así, por el Teorema 2.7, se tiene $x^{p-1} \equiv 1 \pmod p$. Esta contradicción demuestra que $x^2 \equiv -1 \pmod p$ no tiene solución en este caso.

**Problemas**

1. Hacer una lista de todos los enteros $x$ en el intervalo $1 \leqq x \leqq 100$ que satisfagan $x \equiv 7 \pmod{17}$.
2. Mostrar un sistema completo de residuos módulo 17 compuesto enteramente de múltiplos de 3.
3. Mostrar un sistema reducido de residuos para el módulo 12; para 30.
4. Obsérvese que, si un entero $x$ es par, debe satisfacer la congruencia $x \equiv 0 \pmod 2$. Si un entero $y$ es impar, ¿qué congruencia satisface? ¿Qué congruencia satisface un entero $z$ de la forma $6k + 1$?
5. Escribir una sola congruencia que sea equivalente al par de congruencias $x \equiv 1 \pmod 4$, $x \equiv 2 \pmod 3$.
6. Probar que si $p$ es un primo y $a^2 \equiv b^2 \pmod p$, entonces $p|(a + b)$ o bien $p|(a - b)$.
7. Demostrar que si $f(x)$ es un polinomio con coeficientes enteros y si $f(a) \equiv k \pmod m$, entonces $f(a + tm) \equiv k \pmod m$ para todo entero $t$.
8. Probar que cualquier número que sea un cuadrado debe tener como dígito de las unidades a cualquiera de los siguientes: 0, 1, 4, 5, 6, 9.
9. Probar que cualquier cuarta potencia debe tener como dígito de las unidades a 0, 1, 5 o bien 6.
10. Evaluar $\phi(m)$ para $m = 1, 2, 3, \ldots, 12$.
11. Encontrar el menor entero positivo $x$ tal que $13|(x^2 + 1)$.
12. Probar que 19 no es un divisor de $4n^2 + 4$ para cualquier entero $n$.
13. Mostrar un sistema reducido de residuos módulo 7 compuesto enteramente por potencias de 3.
14. Resolver $3x \equiv 5 \pmod{11}$ por el método del Corolario 2.9.
15. Ilustrar la demostración del Teorema 2.10 para $p = 11$ y $p = 13$ determinando realmente los pares de enteros asociados.
16. Los enteros 12, 23, 34, 45, 56 son congruentes a 1 módulo 11. Para resolver $5x \equiv 1 \pmod{11}$ simplemente se observa que $45 = 5 \times 9$ y de aquí que $x = 9$ es una solución. Resolver $ax \equiv 1 \pmod{11}$ para $a = 2, 3, \ldots, 10$.
17. Probar que $n^6 - 1$ es divisible entre 7 si $(n, 7) = 1$.
18. Probar que $n^7 - n$ es divisible entre 42, para cualquier entero $n$.
19. Probar que $n^{12} - 1$ es divisible entre 7 si $(n, 7) = 1$.
20. Probar que $n^{6k} - 1$ es divisible entre 7 si $(n, 7) = 1$, siendo $k$ cualquier entero positivo.
21. Probar que $n^{13} - n$ es divisible entre 2, 3, 5, 7 y 13 para cualquier entero $n$.
22. Probar que $n^{12} - a^{12}$ es divisible entre 13 si $n$ y $a$ son primos para 13.

23. Probar que $n^{12} - a^{12}$ es divisible entre 91 si $n$ y $a$ son primos para 91.
24. Probar que $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es un entero para todo entero $n$.
25. ¿Cuál es el último dígito en la representación decimal ordinaria de $3^{400}$?
*Sugerencia:* Por el teorema de Fermat, $3^4 \equiv 1 \pmod 5$ y esto con $3^4 \equiv 1 \pmod 2$ implica que $3^4 \equiv 1 \pmod{10}$. De aquí que $3^{4n} \equiv 1 \pmod{10}$ para cualquier $n \geqq 1$.
26. ¿Cuál es el último dígito en la representación decimal ordinaria de $2^{400}$?
27. ¿Cuáles son los dos últimos dígitos en la representación decimal ordinaria de $3^{400}$? *Sugerencia:* aplicar el Teorema 2.8 para establecer que $3^{20} \equiv 1 \pmod{25}$. Además $3^2 \equiv 1 \pmod 4$ de manera que $3^{20} \equiv 1 \pmod 4$, de donde $3^{20} \equiv 1 \pmod{100}$.
28. Demostrar que $-(m-1)/2, -(m-3)/2, \ldots, (m-3)/2, (m-1)/2$ es un sistema completo de residuos módulo $m$ si $m$ es impar y que $-(m-2)/2, -(m-4)/2, \ldots, (m-2)/2, m/2$ es un sistema completo de residuos módulo $m$ si $m$ es par.
29. Demostrar que $2, 4, 6, \ldots, 2m$ es un sistema completo de residuos módulo $m$ si $m$ es impar.
30. Demostrar que $1^2, 2^2, \ldots, m^2$ no es un sistema completo de residuos módulo $m$ si $m > 2$.
31. Si $n$ es compuesto, $n > 4$, probar que $(n-1)! \equiv 0 \pmod n$.
32. Demostrar que un entero $m > 1$ es primo y solamente si $m$ divide a $(m-1)! + 1$.
33. Para los enteros positivos $a, m, n$ con $m \neq n$, probar que

$$(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{si } a \text{ es par,} \\ 2, & \text{si } a \text{ es impar.} \end{cases}$$

*Sugerencia*: si $p$ es un divisor común, $a^{2^m} \equiv -1 \pmod p$. Elevar esto a la potencia $2^{n-m}$, suponiendo $m < n$.
34. Para $m$ impar, probar que la suma de los elementos de cualquier sistema completo de residuos módulo $m$ es congruente a cero módulo $m$; probar el resultado análogo para cualquier sistema reducido de residuos para $m > 2$.
35. Encontrar todos los conjuntos de enteros positivos $a, b, c$ que satisfagan simultáneamente las tres congruencias $a \equiv b \pmod c$, $b \equiv c \pmod a$, $c \equiv a \pmod b$. *Sugerencia:* si $a, b, c$ es un conjunto de ese tipo, también lo es $ka, kb, kc$ para cualquier entero positivo $k$. De aquí que es suficiente con determinar todos los conjuntos "primitivos" con la propiedad $(a, b, c) = 1$. También del mismo modo, no se pierde generalidad al suponer que $a \leqq b \leqq c$.
36. Encontrar todas las tripletas $a, b, c$ de enteros diferentes de cero tales que $a \equiv b \pmod{|c|}$, $b \equiv c \pmod{|a|}$, $c \equiv a \pmod{|b|}$.
37. Si $p$ es un primo impar, probar que:

$$1^2 \cdot 3^2 \cdot 5^2 \cdots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod p$$

y

$$2^2 \cdot 4^2 \cdot 6^2 \cdots (p-1)^2 \equiv (-1)^{(p+1)/2} \pmod p.$$

38. Probar que $(a+b)^p \equiv a^p + b^p \pmod p$.
39. Si $r_1, r_2, \ldots, r_{p-1}$ es cualquier sistema reducido de residuos módulo primo $p$, probar que

$$\prod_{j=1}^{p-1} r_j \equiv -1 \pmod{p}.$$

40. Si $r_1, r_2, \ldots, r_p$ y $r_1', r_2', \ldots, r_p'$ son dos sistemas completos cualesquiera de residuos módulo primo $p > 2$, probar que el conjunto $r_1r_1', r_2r_2', \ldots, r_pr_p'$ no puede ser un sistema completo de residuos módulo $p$.
41. Si $p$ es cualquier primo que no sea 2 o bien, 5, probar que $p$ divide un número infinito de los enteros 9, 99, 999, 9999, . . . . Si $p$ es cualquier primo que no sea 2 o bien 5, probar que $p$ divide a un número infinito de los enteros 1, 11, 111, 1111, . . . .
42. Si $p$ es un primo y si $h + k = p - 1$ con $h \geqq 0$ y $k \geqq 0$, probar que $h!k! + (-1)^h \equiv 0 \pmod{p}$.
43. Para cualquier primo $p$, si $a^p \equiv b^p \pmod{p}$, probar que $a^p \equiv b^p \pmod{p^2}$.
44. Dado un entero $n$, probar que existe un entero $m$ el cual para la base diez contiene solamente los dígitos 0 y 1 tales que $n|m$. Probar que se cumple lo mismo para los dígitos 0 y 2, o bien 0 y 3, . . . , o bien 0 y 9 pero no para otro par de dígitos.
45. Si $n$ es compuesto probar que $(n-1)! + 1$ no es una potencia de $n$.
46. Si $1 \leqq k < n - 1$ probar que $(n-1)^2 \nmid (n^k - 1)$.
47. Si $p$ es un primo, probar que $(p-1)! + 1$ es una potencia de $p$ si y solamente si $p = 2$, 3 o bien 5. *Sugerencia:* si $p > 5$, $(p-1)!$ tiene los factores 2, $p - 1$ y $(p-1)/2$ y por lo tanto $(p-1)!$ es divisible entre $(p-1)^2$.
48. Probar que $$\prod_{\substack{1 \leq x \leq n \\ (x,n) = (x+1,n) = 1}} x \equiv 1 \pmod{n} \quad \text{si } n > 2.$$

    El símbolo de la izquierda denota el producto de todos los enteros positivos $x$ menores que o iguales a $n$ tales que tanto $x$ como $x + 1$ son relativamente primos para $n$.
49. Probar que existe un número infinito de primos de la forma $4n + 1$.
50. Probar que $(p-1)! \equiv p - 1 \pmod{1 + 2 + \cdots + (p-1)}$ si $p$ es primo.
51. Considérese que $\tau(n)$ denota el número de divisores positivos de $n$ inclusive $n$, para los enteros positivos $n$. Para $d$ tal que $d|n$, $1 \leqq d \leqq \sqrt{n}$, parear $d$ con $n/d$ para probar que $\tau(n) < 2\sqrt{n}$.

## 2.2 Solución de congruencias

En analogía con la solución de ecuaciones algebraicas, es natural considerar el problema de resolver una congruencia. En el resto de este capítulo, el símbolo $f(x)$ denotará un polinomio con coeficientes enteros y se escribirá $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$. Si $u$ es un entero tal que $f(u) \equiv 0 \pmod{m}$ entonces se dice que $u$ es una solución de la congruencia $f(x) \equiv 0 \pmod{m}$. El que un entero sea o no una solución de una congruencia depende tanto del módulo $m$ como del polinomio $f(x)$. Si el entero $u$ es una solución de $f(x) \equiv 0 \pmod{m}$ y si $v \equiv u$

(mod $m$), el Teorema 2.2 demuestra que $v$ también es una solución. Debido a esto se dice que $x \equiv u \pmod{m}$ es una solución de $f(x) \equiv 0 \pmod{m}$, dando a entender que todo entero congruente a $u$ módulo $m$ satisface $f(x) \equiv 0 \pmod{m}$. Por ejemplo, la congruencia $x^2 - x + 4 \equiv 0 \pmod{10}$ tiene la solución 3. También tiene la solución 8. Puede decirse que $x \equiv 3 \pmod{10}$ y $x \equiv 8 \pmod{10}$ son soluciones. En este caso, puesto que $8 \equiv 3 \pmod{5}$, incluso puede decirse que $x \equiv 3 \pmod{5}$ es una solución. En el caso general, si $f(x) \equiv 0 \pmod{m}$ tiene una solución $u$, tiene un número infinito de soluciones— todos los enteros $v$ tales que $v \equiv u \pmod{m}$. Es más razonable considerar las soluciones en una forma diferente. No se considerará $v$ diferente de $u$ si $v \equiv u$ (mod $m$). En el ejemplo no se consideraron separadamente 3 y 13. Sin embargo, se consideraron tanto 3 como 8 ya que $3 \not\equiv 8 \pmod{10}$.

**Definición 2.4** *Considérese que $r_1, r_2, \ldots, r_m$ denota un sistema completo de residuos módulo m. El número de soluciones de $f(x) \equiv 0 \pmod{m}$ es el número de los $r_i$ tales que $f(r_i) \equiv 0 \pmod{m}$.*

Es evidente, con base en el Teorema 2.2, que el número de soluciones es independiente de la selección del sistema ompleto de residuos. Además, el número de soluciones no puede exceder al módulo $m$. Si $m$ es pequeño, es muy sencillo calcular $f(r_i)$ para cada uno de los $r_i$ y determinar así el número de soluciones. En el ejemplo anterior, la congruencia tiene precisamente dos soluciones. Algunos otros ejemplos son

$x^2 + 1 \equiv 0 \pmod{7}$ no tiene soluciones

$x^2 + 1 \equiv 0 \pmod{5}$ tiene dos soluciones

$x^2 - 1 \equiv 0 \pmod{8}$ tiene cuatro soluciones.

**Definición 2.5** *Sea $f(x) \not\equiv a_0x^n + a_1x^{n-1} + \cdots + a_n$. Si $a_0 \not\equiv 0 \pmod{m}$ el grado de la congruencia $f(x) \equiv 0 \pmod{m}$ es $n$. Si $a_0 \equiv 0 \pmod{m}$, sea $j$ el menor entero positivo tal que $a_j \not\equiv 0 \pmod{m}$; entonces el grado de la congruencia es $n - j$. Si no existe tal entero $j$, esto es, si todos los coeficientes de $f(x)$ son múltiplos de $m$, no se asigna grado a la congruencia.*

Debe observarse que el grado de la congruencia $f(x) \equiv 0 \pmod{m}$ no es lo mismo que el grado del polinomio $f(x)$. El grado de la congruencia depende del módulo; el grado del polinomio no depende del módulo. Así, por ejemplo, si $g(x) = 6x^3 + 3x^2 + 1$, entonces $g(x) \equiv 0 \pmod{5}$ es de grado 3 y $g(x) \equiv 0 \pmod{2}$ es de grado 2, mientras que $g(x)$ es de grado 3.

**Teorema 2.12** *Si $d|m$, $d > 0$, y si $u$ es una solución de $f(x) \equiv 0 \pmod{m}$, entonces $u$ es una solución de $f(x) \equiv 0 \pmod{d}$.*

*Demostración.* Esta se deduce directamente a partir del Teorema 2.1*e*.

**Problemas**

1. Si $f(x) \equiv 0 \pmod p$ tiene exactamente $j$ soluciones y $g(x) \equiv 0 \pmod p$ no tiene soluciones, probar que $f(x)g(x) \equiv 0 \pmod p$ tiene exactamente $j$ soluciones.
2. Denotando por $N(k)$ el número de soluciones de $f(x) \equiv k \pmod m$, probar que $\sum_{k=1}^{m} N(k) = m$.
3. Si una congruencia $f(x) \equiv 0 \pmod m$ tiene $m$ soluciones, probar que cualquier entero es una solución. (En tal caso la congruencia en ocasiones recibe el nombre de congruencia idéntica).
4. El hecho de que el producto de tres enteros consecutivos cualesquiera sea divisible entre 3 conduce a la congruencia idéntica $x(x+1)(x+2) \equiv 0 \pmod 3$. Generalizar este hecho y escribir una congruencia idéntica módulo $m$.

## 2.3 Congruencias de grado uno

Cualquier congruencia de grado 1 puede ponerse en la forma $ax \equiv b \pmod m$, $a \not\equiv 0 \pmod m$. A partir del Corolario 2.9 se ve que si $(a, m) = 1$, entonces $ax \equiv b \pmod m$ tiene exactamente una solución, $x \equiv x_1 \pmod m$.

Denotemos por $g$ al $(a, m)$. Si $ax \equiv b \pmod m$ tiene una solución $u$, entonces $b \equiv au \pmod m$ y de aquí que $b \equiv au \equiv 0 \pmod g$. Por lo tanto, $ax \equiv b \pmod m$ no tiene solución si $g \nmid b$. Sin embargo, si $g|b$ entonces, para un entero $u$, se cumple $au \equiv b \pmod m$ si y solamente si $(a/g)u \equiv (b/g)$, $\pmod{m/g}$, por el Teorema 2.3*a*. Ahora bien, $(a/g, m/g) = 1$ y la congruencia $(a/g)x \equiv (b/g) \pmod{m/g}$ tiene precisamente una solución $x \equiv x_1 \pmod{m/g}$. En otras palabras, las soluciones de $ax \equiv b \pmod m$ son los enteros $u$ tales que $u \equiv x_1 \pmod{m/g}$, es decir, $u = x_1 + t(m/g)$, $t = 0, \pm 1, \pm 2, \ldots$. Si a $t$ se le dan los valores $0, 1, \ldots, g-1$, entonces $u$ toma los valores $g$, ningún par de los cuales son congruentes módulo $m$. Si a $t$ se le da cualquier otro valor, el $u$ correspondiente será congruente módulo $m$ a uno de estos valores $g$. Así que las soluciones de $ax \equiv b \pmod m$ son $x \equiv x_1 + t(m/g) \pmod m$, $0 \leqq t \leqq g-1$.

***Teorema* 2.13** *Denotemos por g al* $(a, m)$. *Entonces* $ax \equiv b \pmod m$ *no tiene soluciones si* $g \nmid b$. *Si* $g|b$, *tiene g soluciones* $x \equiv (b/g)x_0 + t(m/g) \pmod m$, $t = 0, 1, \ldots, g-1$, *donde* $x_0$ *es cualquier solución de* $(a/g)x \equiv 1 \pmod{m/g}$.

*Demostración.* Este teorema se concluye a partir de lo que ya ha sido probado puesto que $(a/g)x \equiv 1 \pmod{m/g}$ tiene una solución $x_0$ y, en

consecuencia, $x_1 = (b/g)x_0$ es una solución de $(a/g)x \equiv (b/g)$ (mod $m/g$).

Para números razonablemente pequeños, con frecuencia puede obtenerse la solución de una congruencia por inspección o bien, probando todos los enteros de un sistema completo de residuos módulo $m$. Sin embargo, si los números son grandes, la solución numérica real de una congruencia de la forma $ax \equiv b$ (mod $m$) puede ser muy larga. La parte más complicada es resolver congruencias $ax \equiv 1$ (mod $m$) con $(a, m) = 1$. La solución tal y como se da en la demostración del Corolario 2.9 generalmente no es práctica. Se han desarrollado varios métodos especiales de solución, pero quizá el método más general es usar el algoritmo de Euclides. Usando el Teorema 1.11 se determina $g = (a, m)$ y al mismo tiempo se obtienen los enteros $u$ y $v$ tales como $au + mv = g$. Entonces tome $u$ como $x_0$ en el Teorema 2.13 y el resto es fácil.

Otra forma de resolver una congruencia de grado 1 es mediante la factorización del módulo como $m = \prod_{i=1}^{k} p_i^{e_i}$. Escribiendo $m_i = p_i^{e_i}$ se observa que los $m_i$ son relativamente primos en pares y que $[m_1, m_2, \cdots, m_k] = m$. Del Teorema 2.3c se ve que el problema de resolver $ax \equiv b$ (mod $m$) es equivalente a resolver el conjunto de congruencias $ax \equiv b$ (mod $m_i$), $i = 1, 2, \cdots, k$, simultáneamente. Las congruencias individuales $ax \equiv b$ (mod $m_i$) pueden resolverse más fácilmente en virtud de que sus módulos $m_i$ son menores que $m$. Supóngase que las congruencias $ax \equiv b$ (mod $m_i$) tienen las soluciones $x \equiv u_i$ (mod $m_i$). Todavía falta el problema de encontrar la solución simultánea $x$ del conjunto de congruencias. La demostración del siguiente teorema proporcionará la forma de hacerlo.

**Teorema 2.14** *Teorema chino del residuo. Supóngase que* $m_1, m_2, \ldots, m_r$ *denotan* $r$ *enteros positivos los cuales son primos relativos en pares y supóngase que* $a_1, a_2, \ldots, a_r$ *denotan* $r$ *enteros cualesquiera. Entonces las congruencias* $x \equiv a_i$ (mod $m_i$), $i = 1, 2, \ldots, r$, *tienen soluciones comunes. Dos soluciones cualesquiera son congruentes módulo* $m_1 m_2 \ldots m_r$.

*Observación.* Si los módulos $m_1, m_2, \ldots, m_r$ no son primos relativos en pares, no puede haber solución de las congruencias. Las condiciones necesaria y suficiente se dan en el problema 14($c$) del siguiente conjunto de problemas.

*Demostración.* Escribiendo $m = m_1 m_2 \ldots m_r$ se ve que $m/m_j$ es un entero y que $(m/m_j, m_j) = 1$. Por lo tanto, por el Corolario 2.9, existen los enteros $b_j$ tales que $(m/m_j)b_j \equiv 1$ (mod $m_j$). Evidentemente $(m/m_j)b_j \equiv 0$ (mod $m_i$) si $i \neq j$. Ahora bien, si se define $x_0$ como

(2.1) $$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j$$

se tiene

$$x_0 \equiv \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j \equiv \frac{m}{m_i} b_i a_i \equiv a_i \pmod{m_i}$$

de modo que $x_0$ es una solución común de las congruencias originales.

Si $x_0$ así como $x_1$ son soluciones comunes de $x \equiv a_i \pmod{m_i}$, $i = 1, 2, \ldots, r$, entonces $x_0 \equiv x_1 \pmod{m_i}$ para $i = 1, 2, \ldots, r$ y de aquí que $x_0 \equiv x_1 \pmod{m}$, por el Teorema 2.3*c*. Esto completa la demostración.

La demostración de este teorema nos proporciona un método eficiente para resolver cierto tipo de problemas. Como un ejemplo, encontremos todos los enteros que tienen los residuos 1 o bien 2 cuando se dividen entre 3, 4 o bien 5. En otras palabras, deben encontrarse las soluciones comunes de $x \equiv 1$ o bien $2 \pmod 3$, $x \equiv 1$ o bien $2 \pmod 4$, $x \equiv 1$ o bien $2 \pmod 5$. Se tiene $m_1 = 3$, $m_2 = 4$, $m_3 = 5$, $m = 60$ y cada uno de los $a_i$ es 1 o bien 2. Para encontrar $b_1$ se resuelve $(60/3)b_1 \equiv 1 \pmod 3$; esto es $20b_1 \equiv 1 \pmod 3$, lo cual es lo mismo que $-b_1 \equiv 1 \pmod 3$. Puede tomarse $b_1 = -1$ y entonces tener $(m/m_1)b_1 = -20$. De modo semejante se obtiene $b_2 = -1$ $(m/m_2)b_2 = -15$. Para $b_3$ se tiene $12b_3 \equiv 1 \pmod 5$, $2b_3 \equiv 1$, $4b_3 \equiv 2$, $-b_3 \equiv 2$ y puede tomarse $b_3 = -2, (m/m_3)b_3 = -24$. Usando (2.1) simplemente deben sustituirse los valores de los $a_i$ en $x \equiv -20a_1 - 15a_2 - 24a_3 \pmod{60}$. Haciendo esto se obtienen los valores dados en la siguiente tabla

| $a_1$ | $a_2$ | $a_3$ | $x$ (mód 60) |
|---|---|---|---|
| 1 | 1 | 1 | $-20 - 15 - 24 \equiv -59 \equiv 1$ |
| 1 | 1 | 2 | $-20 - 15 - 48 \equiv -83 \equiv -23$ |
| 1 | 2 | 1 | $-20 - 30 - 24 \equiv -74 \equiv -14$ |
| 2 | 1 | 1 | $-40 - 15 - 24 \equiv -79 \equiv -19$ |
| 2 | 2 | 1 | $-40 - 30 - 24 \equiv -94 \equiv 26$ |
| 2 | 1 | 2 | $-40 - 15 - 48 \equiv -103 \equiv 17$ |
| 1 | 2 | 2 | $-20 - 30 - 48 \equiv -98 \equiv 22$ |
| 2 | 2 | 2 | $-40 - 30 - 48 \equiv -118 \equiv 2$ |

Los enteros que tienen residuos 1 o bien 2 cuando se dividen entre 3, 4, 5 están dados por $x \equiv 1, 2, 17, 22, 26, -14, -19, -23 \pmod{60}$.

**Problemas**

1. Encontrar todas las soluciones de las congruencias

$a$) $20x \equiv 4 \pmod{30}$;
$b$) $20x \equiv 30 \pmod 4$;
$c$) $353x \equiv 254 \pmod{400}$.

2. ¿Cuántas soluciones existen para cada una de las siguientes congruencias?
$a$) $15x \equiv 25 \pmod{35}$;
$b$) $15x \equiv 24 \pmod{35}$;
$c$) $15x \equiv 0 \pmod{35}$.
3. Encontrar el menor entero positivo (excepto $x = 1$) que satisfaga simultáneamente las siguientes congruencias: $x \equiv 1 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 1 \pmod 7$.
4. Encontrar todos los enteros que satisfagan simultáneamente: $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 5 \pmod 2$.
5. Resolver el conjunto de congruencias: $x \equiv 1 \pmod 4$, $x \equiv 0 \pmod 3$, $x \equiv 5$ mod 7).
6. Encontrar todos los enteros que dan los residuos 1, 2, 3 cuando se dividen entre 3, 4, 5, respectivamente.
7. Si $a$ se selecciona al azar de 1, 2, 3, . . . , 14 y $b$ se selecciona al azar de 1, 2, 3, . . . , 15, ¿cuál es la probabilidad de que $ax \equiv b \pmod{15}$ tenga por lo menos una solución? ¿Exactamente una solución?
8. Dado cualquier entero positivo $k$, probar que existen $k$ enteros consecutivos cada uno de los cuales es divisible entre un cuadrado $> 1$.
9. Si $x_2$ es una solución de la congruencia $ax \equiv b \pmod m$ (tal vez obtenida mediante la aplicación del algoritmo de Euclides a $a$ y $m$), probar que $x \equiv x_2 + t(m/g) \pmod m$ proporciona todas las soluciones conforme $t$ recorre todos los valores $0, 1, \cdots, g - 1$, donde $g$ se define como $g = (a, m)$.
10. Supóngase que $(a, m) = 1$ y que $x_1$ denota una solución de $ax \equiv 1$ (mod $m$). Para $s = 1, 2, \cdots$, sea $x_s = 1/a - (\text{v}/a)(1 - ax_1)^s$. Probar que $x_s$ es un entero y que es una solución de $ax \equiv 1 \pmod{m^s}$.
11. Supóngase que $(a, m) = 1$. Si $a = \pm 1$, la solución de $ax \equiv 1 \pmod{m^s}$ obviamente es $x \equiv a \pmod{m^s}$. Si $a = \pm 2$, entonces $m$ es impar y $x \equiv \frac{1}{2}(1 - m^s)\frac{1}{2}a \pmod{m^s}$ es la solución de $ax \equiv 1 \pmod{m^s}$. Usar el resultado del problema 11 para demostrar que, para cualquier otra $a$, la solución de $ax \equiv 1 \pmod{m^s}$ es $x \equiv k \pmod{m^s}$ donde $k$ es el entero más próximo a $-(1/a)\ (1 - ax_1)^s$.
12. Resolver $3x \equiv 1 \pmod{125}$ mediante el Problema 12, tomando $x_1 = 2$.
13. Sean $m_1, m_2, \ldots, m_r$ primos relativos en pares. Suponiendo que cada una de las congruencias $b_i x \equiv a_i \pmod{m_i}$, $i = 1, 2, \ldots, r$, tiene solución, probar que las congruencias tienen una solución simultánea.
14. $a$) Considérese el conjunto de congruencias $x \equiv a_i$ (mol $p^{e_i}$), $i = 1, 2, \ldots, r$ con $e_1 \geqq e_2 \geqq \ldots \geqq e_r$. Probar que $x = a_1$ es una solución simultánea de estas congruencias si $p^{e_i} | (a_1 - a_i)$ para $i = 2, 3, \ldots, r$.
$b$) Sea $p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ la factorización canónica de $m$. Probar que cualquier solución simultánea del conjunto de congruencias $x \equiv a \pmod{p_i^{e_i}}$, $i = 1, 2, \ldots, k$, es una solución de $x \equiv a \pmod m$.
$c$) Probar que el conjunto de congruencias $x \equiv a_i \pmod{m_i}$, $i = 1, 2, \ldots, n$, tiene una solución simultánea si, y solamente si, $(m_i, m_j) | (a_i - a_j)$ se cumple par atodo par de módulos, esto es, para todo par de subíndices $i$, $j$ tales que $1 \leqq i < j \leqq n$. Dos soluciones cualesquiera son congruentes módulo $[m_1, m_2, \ldots, m_n]$

15. Sea $(a, b) = 1$ y $c > 0$. Probar que existe un entero $x$ tal que $(a + bx, c) = 1$.
16. Considérese un cuadrado dividido en $n^2$ cuadrados iguales. Numérense las columnas de cuadrados pequeños $1, 2, \ldots, n$, de izquierda a derecha. De modo semejante, numérense las hileras horizontales $1, 2, \ldots, n$ y denótese por $\{c, r\}$ el cuadrado pequeño que se encuentra en la $c$-ésima columna y $r$-ésima hilera.
Sean $a_0$, $b_0$, $a$, $b$, $\alpha$, $\beta$ enteros positivos menores que o iguales a $n$ y tales que $(a, n) = (b, n) = (\alpha, n) = (\beta, n) = 1$. Escribir 1 en el cuadrado $\{a_0, b_0\}$. Entonces contar $a$ columnas hacia la derecha y $b$ hileras hacia arriba de este cuadrado. Si este procedimiento lleva hacia afuera del cuadrado grande, cuéntese como si el cuadrado grande se enrollara en un cilindro. Así se llegará al cuadrado $\{a_0 + a, b_0 + b\}$ o bien $\{a_0 + a - n, b_0 + b\}$ o bien $\{a_0 + a, b_0 + b - n\}$ o bien $\{a_0 + a - n, b_0 + n\}$, el que sea realmente uno de los pequeños cuadrados. Escribir 2 en este cuadrado. Contar $a$ hacia la derecha y $b$ hacia arriba de 2 e insértese 3 en el cuadrado. Continuar hasta que se haya escrito $1, 2, 3, \cdots, n$. Probar que se habrá escrito $m$ en $\{x_m, y_m\}$ donde $x_m$ y $y_m$ están unívocamente determinados por

$$x_m \equiv a_0 + a(m - 1) \pmod n, \quad 1 \leqq x_m \leqq n$$
$$y_m \equiv b_0 + b(m - 1) \pmod n, \quad 1 \leqq y_m \leqq n, 1 \leqq m \leqq n.$$

También demostrar que todos estos cuadrados $\{x_m, y_m\}$ son diferentes pero que continuando el proceso un paso más se colocaría $n + 1$ en $\{a_0, b_0\}$ el cual ya está ocupado por 1.

Ahora, habiendo alcanzado $\{a_0, b_0\}$ una vez más, contar $\alpha$ hacia la derecha y $\beta$ hacia arriba y escribir $n + 1$ en este cuadrado, el cual puede estar o puede no estar ya ocupado. Entonces regrésese al proceso original con el peso $a, b$ para insertar $n + 2$, $n + 3, \ldots, 2n$. Continúese en esta forma, usando el paso adicional $\alpha$, $\beta$ precisamente para $n + 1$, $2n + 1, \ldots, (n - 1)n + 1$ y acabando cuando se haya insertado $n^2$.

Para $1 \leqq m \leqq n^2$, probar que $m$ está en $\{x_m, y_m\}$ donde

$$x_m \equiv a_0 + a(m - 1) + \alpha \left[\frac{m - 1}{n}\right] \pmod n, \quad 1 \leqq x_m \leqq n,$$

$$y_m \equiv b_0 + b(m - 1) + \beta \left[\frac{m - 1}{n}\right] \pmod n, \quad 1 \leqq y_m \leqq n,$$

y $\left[\frac{m - 1}{n}\right]$ es el cociente cuando $n$ se divide en $m - 1$.

También probar que si $(a\beta - b\alpha, n) = 1$ entonces cada cuadrado contiene uno y solamente un entero $m$, $1 \leqq m \leqq n^2$.

De aquí en adelante supóngase que $(a\beta - b\alpha, n) = 1$. Escribiendo $m - 1 = qn + s$, $0 \leqq s \leqq n - 1$, demostrar que las anotaciones de la $c$-ésima columna son precisamente los $m = qn + s + 1$ para los cuales $0 \leqq q \leqq n - 1$, $0 \leqq s \geqq n - 1$ y $as \equiv c - a_0 - \alpha q \pmod n$. Probar que existe uno y solamente un $s$ para cada $q$ y que cada $s$ es distinto a todos los demás. Entonces demostrar que

$$\text{Suma de los } m \text{ en la } c\text{-ésima columna} = \sum_{q=0}^{n-1} qn + \sum_{s=0}^{n-1} s + n = \frac{n(n^2 + 1)}{2}.$$

Probar lo mismo para la suma en una hilera. Dado que $n(n^2 + 1)/2$ es independiente de $c$, las sumas en cada hilera y en cada columna son las mismas y, por tal motivo, este arreglo cuadrado de los enteros recibe el nombre de cuadrado mágico.

Obsérvese que el cuadrado inicial $\{a_0, b_0\}$ no está sujeto a condiciones. Las únicas condiciones esenciales son que $a$, $b$, $\alpha$, $\beta$, $a\beta - b\alpha$ sean relativamente primos para $n$. Demostrar que estas condiciones no pueden ser satisfechas si $n$ es par. Sin embargo, para $n$ impar, los valores $a = b = \alpha = 1$, $\beta = 2$ siempre dan un cuadrado mágico.

## 2.4 La función $\phi(n)$

Regresaremos a la discusión de la solución de las congruencias en la próxima sección. En esta sección aplicaremos el teorema chino del residuo para obtener una importante propiedad de la función $\phi(n)$ de la Definición 2.3.

**Teorema 2.15.** *Denotemos por $m$ y $n$ dos enteros positivos y primos relativos. Entonces $\phi(nm) = \phi(n)\,\phi(m)$.*

*Demostración.* Denotemos $\phi(m)$ por $j$ y sea $r_1, r_2, \cdots, r_j$ un sistema reducido de residuos módulo $m$. De modo semejante, escribir $k$ por $\phi(n)$ y sea $s_1, s_2, \cdots, s_k$ un sistema reducido de residuos módulo $n$. Si $x$ es un sistema reducido de residuos módulo $mn$, entonces $(x, m) = (x, n) = 1$ y de aquí que $x \equiv r_h \pmod{m}$ y $x \equiv s_i \pmod{n}$ para ciertos $h$ e $i$. Inversamente, si $x \equiv r_h \pmod{m}$ y $x \equiv s_i \pmod{n}$ entonces $(x, mn) = 1$. Así que puede obtenerse un sistema reducido de residuos módulo $mn$ determinando todos los $x$ tales que $x \equiv r_h \pmod{m}$ y $x \equiv s_i \pmod{n}$ para ciertos $h$ e $i$. De acuerdo con el teorema chino del residuo, cada par $h, i$ determina un solo $x$ módulo $mn$. Evidentemente, diferentes pares $h, i$ proporcionan diferentes $x$ módulo $mn$. Existen $jk$ de estos pares. Por lo tanto, un sistema reducido de residuos módulo $mn$ contiene $jk = \phi(m)\phi(n)$ números y se tiene $\phi(mn) = \phi(m)\phi(n)$.

Es esencial que $m$ y $n$ sean primos relativos. En efecto, $\phi(2) = 1$ y $\phi(2^2) = 2 \neq \phi(2)\phi(2)$.

**Teorema 2.16.** *Si $n > 1$ entonces $\phi(n) = n \prod_{p|n} (1 - 1/p)$. También $\phi(1) = 1$.*

*Observación.* El símbolo $\prod_{p|n}$ denota el producto del conjunto de todos los primos que dividen a $n$. Así que si $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ en forma canónica, entonces $\prod_{p|n} (1 - 1/p)$ significa $\prod_{j=1}^{r} (1 - 1/p_j)$. Con frecuencia se usará esta notación, tanto como la notación análoga que se refiera a las sumas. También se escribirá $\sum_{d|n}$ para denotar la suma del conjunto de todos los divisores positivos de $n$, primos o no. Además, en ocasiones

usaremos la convención de que una suma vacía es 0, un producto vacío es 1. Habiendo convenido lo anterior, no hubiéramos tenido que tratar $n = 1$ como un caso especial en el establecimiento del teorema.

*Demostración.* Es obvio que $\phi(1) = 1$.

Si $n > 1$ puede escribirse $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ en forma canónica. Ahora bien, $(p_j^{e_j}, p_{j+1}^{e_{j+1}} p_{j+2}^{e_{j+2}} \cdots p_r^{e_r}) = 1$ para $j = 1, 2, \cdots, r - 1$. Aplicando el Teorema 2.15 repetidamente se obtiene

$$\phi(n) = \prod_{j=1}^{r} \phi(p_j^{e_j}).$$

Para calcular $\phi(p^e)$, $p$ primo, recuérdese que $\phi(p^e)$ es el número de enteros $x$ tales que $1 \leqq x \leqq p^e$, $(x, p^e) = 1$. Existen $p^e$ enteros $x$ entre 1 y $p^e$, y deben considerarse todos excepto $p, 2p, 3p, \cdots, p^{e-1}p$. Por lo tanto

$$\phi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right),$$

y de aquí que

$$\phi(n) = \prod_{j=1}^{r} p_j^{e_j}\left(1 - \frac{1}{p_j}\right) = n\prod_{j=1}^{r}\left(1 - \frac{1}{p_j}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right).$$

**Teorema 2.17.** *Para* $n \geqq 1$ *se tiene* $\sum_{d|n} \phi(d) = n$.

*Demostración.* Si $n = p^e$, $p$ primo, entonces

$$\sum_{d|n} \phi(d) = \phi(1) + \phi(p) + \phi(p^2) + \cdots + \phi(p^e)$$

$$= 1 + (p - 1) + p(p - 1) + \cdots + p^{e-1}(p - 1)$$

$$= p^e = n.$$

Por lo tanto el teorema es verdadero si $n$ es una potencia de un primo. Ahora procederemos por inducción. Supóngase que el teorema se cumple para enteros con $k$ o menos factores primos distintos y considérese cualquier entero $N$ con $k + 1$ factores primos distintos. Denotemos por $p$ uno de los factores primos de $N$ y sea $p^e$ la mayor potencia de $p$ que divide a $N$. Entonces $N = p^e n$, $n$ tiene $k$ factores primos distintos y $(p, n) = 1$. Ahora bien, conforme $d$ varía sobre los divisores de $n$, el conjunto $d, pd, p^2d, \cdots, p^ed$ varía sobre los divisores de $N$. De aquí que se tiene

$$\sum_{d|N} \phi(d) = \sum_{d|n} \phi(d) + \sum_{d|n} \phi(pd) + \sum_{d|n} \phi(p^2d) + \cdots + \sum_{d|n} \phi(p^e d)$$

$$= \sum_{d|n} \phi(d)\{1 + \phi(p) + \phi(p^2) + \cdots + \phi(p^e)\}$$

$$= \sum_{d|n} \phi(d) \sum_{\delta|p^e} \phi(\delta) = np^e = N.$$

En el capítulo 4 se obtendrá una demostración diferente de este teorema. Será independiente de los resultados de esta sección y se encontrará que puede invertirse el orden, que puede empezarse por probar el Teorema 2.17 y obtener, como consecuencia, el Teorema 2.16. Entonces es fácil obtener el Teorema 2.15 a partir del Teorema 2.16.

**Problemas**

1. ¿Para qué valores de $n$ es impar $\phi(n)$?
2. Encontrar el número de enteros positivos $\leqq 3600$ que son primos para 3600.
3. Encontrar el número de enteros positivos $\leqq 3600$ que tienen un factor en común con 3600.
4. Encontrar el número de enteros positivos $\leqq 7200$ que son primos para 3600.
5. Encontrar el número de enteros positivos $\leqq 25200$ que son primos para 3600. (Obsérvese que $25200 = 7 \times 3600$).
6. Si $m$ y $k$ son enteros positivos, probar que el número de enteros positivos $\leqq mk$ que son primos para $m$ es $k\phi(m)$.
7. Demostrar que $\phi(nm) = n\phi(m)$ si todo primo que divide a $n$ también divide a $m$.
8. Si $p$ denota el producto de los primos comunes a $m$ y $n$, probar que $\phi(mn) = P\phi(m)\phi(n)/\phi(P)$. De aquí que si $(m, n) > 1$, probar que $\phi(mn) > \phi(m)\phi(n)$.
9. Si $\phi(m) = \phi(mn)$ y $n > 1$, probar que $n = 2$ y $m$ es impar.
10. Caracterizar el conjunto de enteros positivos $n$ que satisfacen $\phi(2n) = \phi(n)$.
11. Caracterizar el conjunto de enteros positivos que satisfacen $\phi(2n) > \phi(n)$.
12. Probar que existe un número infinito de enteros $n$ de modo que $3 \nmid \phi(n)$.
13. Encontrar todas las soluciones $x$ de $\phi(x) = 24$.
14. Probar que para un entero fijo $n$, la ecuación $\phi(x) = n$ tiene solamente un número finito de soluciones.
15. Encontrar el menor entero positivo $n$ de modo que $\phi(x) = n$ no tenga solución; exactamente dos soluciones; exactamente tres soluciones; exactamente cuatro soluciones. (Se ha conjeturado que no existe entero $n$ tal que $\phi(x) = n$ tenga exactamente una solución, pero éste es un problema no resuelto).
16. Probar que no existe solución de la ecuación $\phi(x) = 14$ y que 14 es el menor entero positivo par con esta propiedad. Además de 14, ¿cuál es el menor entero positivo par siguiente $n$ tal que $\phi(x) = n$ no tiene solución?

17. Probar que para $n \geqq 2$ la suma de todos los enteros positivos menores que $n$ y primos para $n$ es $n\phi(n)/2$.
18. Si $n$ tiene $k$ factores primos impares distintos, probar que $2^k|\phi(n)$.
19. Definir $f(n)$ como la suma de los enteros positivos menores que $n$ y primos para $n$. Probar que $f(m) = f(n)$ implica que $m = n$.
20. Denotemos por $\phi'(n)$ el número de enteros $x$ tales que $1 \leqq x \leqq n$ y $(x, n) = (x + 1, n) = 1$. Probar que

$$\phi'(n) = n \prod_{p|n} \left(1 - \frac{2}{p}\right).$$

21. *a*) Sea $n = \prod_{i=1}^{k} p_i^{a_i}$ la factorización canónica de $n$. Para todo entero positivo $j$, definir

$$e_j(p_i) = \begin{cases} 1 \text{ si } p_i|j \\ 0 \text{ en cualquier otro caso.} \end{cases}$$

Probar que $\sum_{j=1}^{n} e_j(p_1) = n/p_1$ y, más generalmente, que

$$\sum_{j=1}^{n} e_j(p_1)e_j(p_2) \cdots e_j(p_r) = \frac{n}{p_1 p_2 \cdots p_r} \text{ para } 1 \leqq r \leqq k.$$

*b*) Probar que

$$\prod_{i=1}^{k} \{1 - e_j(p_i)\} = \begin{cases} 1 \text{ si } (j, n) = 1 \\ 0 \text{ en cualquier otro caso,} \end{cases}$$

y de aquí que $\phi(n) = \sum_{j=1}^{n} \prod_{i=1}^{k} \{1 - e_j(p_i)\}$.

*c*) Deducir que

$$\phi(n) = \sum_{j=1}^{n} \{1 - e_j(p_1) - e_j(p_2) - \cdots - e_j(p_k) + e_j(p_1)e_j(p_2) + e_j(p_1)e_j(p_3) + \cdots + e_j(p_{k-1})e_j(p_k) - e_j(p_1)e_j(p_2)e_j(p_3) - \text{etc.}\},$$

y así obtener una demostración independiente del Teorema 2.16.
22. Si $d|n$ y $0 < d < n$, probar que $n - \phi(n) > d - \phi(d)$.
23. Probar la siguiente generalización del teorema de Euler:

$$a^m \equiv a^{m-\phi(m)} \pmod m$$

para cualquier entero $a$.

## 2.5 Congruencias de grado superior

No existe método general para resolver las congruencias. Sin embargo, pueden hacerse ciertas reducciones de manera que, finalmente, el problema se transforma en el de resolver congruencias de módulos primos. Puede usarse el método del teorema chino del residuo en el primer paso de esta reducción.

Si $m = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ entonces la congruencia $f(x) \equiv 0 \pmod m$ es equivalente al conjunto de congruencias $f(x) \equiv 0 \pmod{p_i^{e_i}}$, i = 1,

$2, \cdots, r$, en el sentido de que las soluciones de una son soluciones de la otra. Si para algún $j$, $1 \leqq j \leqq r$, la congruencia $f(x) \equiv 0 \pmod{p_j^{e_j}}$ no tiene solución, entonces $f(x) \equiv 0 \pmod{m}$ no tiene solución. Por otra parte, si todas las congruencias $f(x) \equiv 0 \pmod{p^{e_i}}$ tienen soluciones, puede suponerse que la $i$-ésima congruencia tiene exactamente $k_i$ soluciones, digamos $a_i^{(1)}, a_i^{(2)} \cdots, a_i^{(k_i)}$. Ningún par de estas soluciones son congruentes módulo $p_i^{e_i}$, por la Definición 2.4, y toda solución de $f(x) \equiv 0 \pmod{p_i^{e_i}}$ es congruente para algún $a_i^{(j)}$ módulo $p_i$.

Ahora bien, un entero $u$ es una raíz de $f(x) \equiv 0 \pmod{m}$ si y solamente si para cada $i$ existe un $j_i$ tal que $u \equiv a_i^{(j_i)} \pmod{p_i^{e_i}}$. Supuesto que los módulos $p_i^{e_i}$ son relativamente primos en pares, puede aplicarse el teorema chino del residuo. Determinemos los enteros $b_i$ tales que $mp_i^{-e_i}b_i \equiv 1 \pmod{p_i^{e_i}}$ y entonces puede encontrarse $u$ por medio de (2.1);

$$u \equiv \sum_{i=1}^{r} \frac{m}{p_i^{e_i}} b_i a_i^{(j_i)} \quad (\text{mód } m). \tag{2.2}$$

Cuando realmente se resuelve un problema, generalmente es mejor calcular los coeficientes $mp_i^{-e_i}b_i$ en primer lugar puesto que son independientes de la selección de los $j_i$. Entonces es fácil sustituir los diferentes valores de los $a_i^{(j_i)}$ en (2.2) y se resuelve el problema.

Habrá un $u$ diferente módulo $m$ para cada selección de los enteros $j_1, j_2, \cdots, j_r$, y cada $j_i$ puede tomar cualquiera de los valores $k_i$. Por tanto, la congruencia $f(x) \equiv 0 \pmod{m}$ tiene $k_1k_2 \cdots k_r$ soluciones. Dado que $k_i$ es el número de soluciones de $f(x) \equiv 0 \pmod{p_i^{e_i}}$ se tiene el siguiente teorema.

**Teorema 2.18** *Supóngase que $N(m)$ denota el número de soluciones de la congruencia* $f(x) \equiv 0 \pmod{m}$. *Entonces* $N(m) = \prod_{i=1}^{r} N(p_i^{e_i})$ *si $m = p_1^{e_1}p_2^{e_2} \cdots p_r^{e_r}$ es la factorización de $m$.*

Quizá debe hacerse notar que el caso en el cual $N(p_j^{e_j}) = 0$ para algún $j$ no se excluye en el Teorema 2.18.

**Ejemplo.** Resolver $x^2 + x + 7 \equiv 0 \pmod{15}$.

Probando los valores $x = 0, \pm 1, \pm 2$, se encuentra que $x^2 + x + 7 \equiv 0 \pmod{5}$ no tiene solución. Puesto que $15 = 3 \cdot 5$, la congruencia original no tiene solución.

**Ejemplo.** Resolver $x^2 + x + 7 \equiv 0 \pmod{189}$, dado que $x \equiv 4, 13, -5 \pmod{27}$ son las soluciones de $x^2 + x + 7 \equiv 0 \pmod{27}$ y que $x \equiv 0, -1 \pmod{7}$ son las soluciones de $x^2 + x + 7 \equiv 0 \pmod{7}$.

En este ejemplo se tiene $m = 189 = 27 \cdot 7 = 3^3 \cdot 7$, $p_1^{e_1} = 27$, $p_2^{e_2} = 7$, $a_1^{(1)} = 4$, $a_1^{(2)} = 13$, $a_1^{(3)} = -5$, $a_2^{(1)} = 0$, $a_2^{(2)} = -1$. Para encontrar $b_1$ se mul-

tiplica la congruencia $7b_1 \equiv 1 \pmod{27}$ por 4 y se obtiene $b_1 \equiv 28b_1 \equiv 4 \pmod{27}$. Para $b_2$ se tiene $27b_2 \equiv 1 \pmod 7$ la cual proporciona $b_2 \equiv -1 \pmod 7$. Ahora puede escribirse (2.2) como

$$u \equiv 7 \cdot 4a_1^{(j_1)} + 27(-1)a_2^{(j_2)} \equiv 28a_1^{(j_1)} - 27a_2^{(j_2)} \pmod{189}$$

para las raíces $u$ requeridas. Usando los valores conocidos de los $a_i^{(j)}$ rápidamente se encuentra $u \equiv -77, -14, -140, -50, 13, -113 \pmod{189}$.

Si los números hubieran sido mayores podría haberse tenido una mayor dificultad para encontrar $b_1$ y $b_2$. En cualquier caso pueden usarse los métodos mencionados en la sección 2.3.

**Problemas**

1. Resolver las congruencias:

$$x^3 + 2x - 3 \equiv 0 \pmod 9;$$
$$x^3 + 2x - 3 \equiv 0 \pmod 5;$$
$$x^3 + 2x - 3 \equiv 0 \pmod{45}.$$

2. Resolver la congruencia $x^3 + 4x + 8 \equiv 0 \pmod{15}$.
3. Resolver la congruencia $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{503}$ observando que 503 es primo y que el polinomio se factoriza en $(x-1)(x-3)(x-5)$.
4. Resolver la congruencia $x^3 - 9x^2 + 23x - 15 \equiv 0 \pmod{143}$.

## 2.6 Potencia de un primo como módulo

El problema de resolver una congruencia ahora ha sido reducido al de resolver una congruencia cuyo módulo es una potencia de un solo primo.

Si $r$ es una solución de $f(x) \equiv 0 \pmod{p^s}$, entonces $f(r) \equiv 0 \pmod{p^t}$ para $t = 1, 2, \ldots, s$. Sean $x_s^{(1)}, x_s^{(2)}, \ldots, x_s^{(h_s)}$ las soluciones de $f(x) \equiv 0 \pmod{p^s}$. Pueden no haber tales soluciones o pueden haber muchas. Considérense $s \geqq 2$. Si existe una solución $x_s^{(i)}$ entonces existe una solución $x_{s-1}^{(j_i)}$ de $f(x) \equiv 0 \pmod{p^{s-1}}$ tal que $x_s^{(i)} \equiv x_{s-1}^{(j_i)} \pmod{p^{s-1}}$. Por tanto, $x_s^{(i)} \equiv x_{s-1}^{(j_i)} + v_{s-1}p^{s-1} \pmod{p^s}$ para algún entero $v_{s-1}$.

Recordando que $f(x)$ es un polinomio de grado $n$ con coeficientes enteros, se ve que $\frac{1}{1!}f'(x), \frac{1}{2!}f''(x), \ldots$ son polinomios con coeficientes enteros y que $f^{(t)}(x)$ es idénticamente cero para $t > n$. Así que el desarrollo de Taylor de $f(x)$ es finito y se tiene

$$f(x+h) = f(x) + f'(x)h + \frac{1}{2}f''(x)h^2 + \cdots + \frac{1}{n!}f^{(n)}(x)h^n,$$

y entonces

$$0 \equiv f(x_s^{(i)}) \equiv f(x_{s-1}^{(j_i)} + v_{s-1}p^{s-1}) \equiv f(x_{s-1}^{(j_i)}) + f'(x_{s-1}^{(j_i)})v_{s-1}p^{s-1} \pmod{p^s}.$$

Pero $f(x_{s-1}^{(j_i)}) \equiv 0 \pmod{p^{s-1}}$, de modo que se tiene

$$(2.3) \qquad f'(x_{s-1}^{(j_i)})\, v_{s-1} \equiv -\frac{1}{p^{s-1}} f(x_{s-1}^{(j_i)}) \pmod{p}.$$

Inversamente, si

$$(2.4) \qquad f'(x_{s-1}^{(j)})\, v \equiv -\frac{1}{p^{s-1}} f(x_{s-1}^{(j)}) \pmod{p},$$

entonces $f(x_{s-1}^{(j)} + vp^{s-1}) \equiv 0 \pmod{p^s}$. Esto nos muestra cómo encontrar todas las soluciones de $f(x) \equiv 0 \pmod{p^s}$, $s \geqq 2$, si se conocen las de $f(x) \equiv 0 \pmod{p^{s-1}}$. Para cada raíz $x_{s-1}^{(j)}$ se encuentran todas las soluciones $v$ de (2.4) y entonces los enteros $x_{s-1}^{(j)} + vp^{s-1}$ serán las soluciones de $f(x) \equiv 0 \pmod{p^s}$. Por supuesto que puede suceder que no exista $v$ correspondiente para alguna $x_{s-1}^{j}$. En este caso no se tienen soluciones de $f(x) \equiv 0 \pmod{p^s}$ que provengan de esta $x_{s-1}^{(j)}$ particular.

Puede decirse un poco más acerca de las soluciones. Al resolver $f(x) \equiv 0 \pmod{p^s}$, $s \geqq 2$, se empieza con las soluciones $x_1^{(j)}$ de $f(x) \equiv 0 \pmod{p}$. Escogiendo una $x_1^{(j_i)}$ particular, primero debe resolverse (2.3), con $s = 2$, para $v_1$. Para cada $v_1$ se tiene una raíz $x_2^{(k)} \equiv x_1^{(j_i)} + v_1 p \pmod{p^2}$ de $f(x) \equiv 0 \pmod{p^2}$. Usando cada una de estas $x_2^{(k)}$ entonces debe resolverse (2.3) con $s = 3$, $j_1 = k$, para encontrar las soluciones de $f(x) \equiv 0 \pmod{p^3}$. Pero la congruencia para $v_2$ tiene módulo $p$ y $x_2^{(k)} \equiv x_1^{(j_i)} \pmod{p}$, y de aquí que pueda escribirse como

$$f'(x_1^{(j_i)})\, v_2 \equiv -\frac{1}{p^2} f(x_2^{(k)}) \pmod{p}.$$

Esto sucede en cada paso y de aquí que pueda determinarse $v_{s-1}$ de

$$(2.5) \qquad f'(x_1^{(j_i)})\, v_{s-1} \equiv -\frac{1}{p^{s-1}} f(x_{s-1}^{(k)}) \pmod{p}$$

para todas las $x_{s-1}^{(k)}$ que se obtienen al final a partir de la solución $x_1^{(j_i)}$ de $f(x) \equiv 0 \pmod{p}$.

La congruencia (2.5) es una congruencia lineal. Si $f'(x^{(j_i)}) \not\equiv 0 \pmod{p}$, entonces existirá exactamente una $v_{s-1}$ para cada una de las $x_{s-1}^{(k)}$ que se obtienen al final de $x_1^{(j_i)}$. Si $f'(x_1^{(j_i)}) \equiv 0 \pmod{p}$ entonces existirá $p$ o no existirá $v_{s-1}$ de acuerdo como $f'(x_{s-1}^{(k)})/p^{s-1}$ sea o no congruente a 0 módulo $p$.

**Ejemplo.** Resolver $x^2 + x + 7 \equiv 0 \pmod{27}$.

Por tanteos se encuentra que $x \equiv 1 \pmod{3}$ es la única solución de $f(x) \equiv 0 \pmod{3}$ para la presente $f(x)$. Entonces $f'(x) = 2x + 1$ y $f'(1) \equiv 0 \pmod{3}$. Existe solamente una $x_1$ y (2.5) se reduce a

$$0 \equiv -\frac{1}{3^{s-1}} f(x_{s-1}^{(k)}) \pmod{3}.$$

lo cual significa que no existe $v_{s-1}$ si $f(x_{s-1}^{(k)}) \not\equiv 0 \pmod{3^s}$ y que $v_{s-1} \equiv 0, 1, -1 \pmod 3$ si $f(x_{s-1}^{(k)}) \equiv 0 \pmod{3^s}$. Y ahora se encuentra

$$x_1^{(1)} \equiv 1 \pmod 3, f(x_1^{(1)}) = 9, \qquad v_1 \equiv 0, 1, -1 \pmod 3$$
$$x_2^{(1)} \equiv 1 \pmod{3^2}, f(x_2^{(1)}) = 9, \qquad \text{no existe } v_2$$
$$x_2^{(2)} \equiv 4 \pmod{3^2}, f(x_2^{(2)}) = 27, \qquad v_2 \equiv 0, 1, -1 \pmod 3$$
$$x_2^{(3)} \equiv -2 \pmod{3^2}, f(x_2^{(3)}) = 9, \qquad \text{no existe } v_2$$
$$x_3^{(1)} \equiv 4 \pmod{3^3}$$
$$x_3^{(2)} \equiv 13 \pmod{3^3}$$
$$x_3^{(3)} \equiv -5 \pmod{3^3}.$$

**Ejemplo.** Resolver $x^2 + x + 7 \equiv 0 \pmod{3^4}$.
Continuando con el ejemplo anterior, se encuentra

$$f(x_3^{(1)}) = 27, \quad f(x_3^{(2)}) = 189, \quad f(x_3^{(3)}) = 27.$$

La congruencia no tiene solución dado que $27 \not\equiv 0$, $189 \not\equiv 0$, $\pmod{3^4}$.

**Ejemplo.** *Resolver* $x^2 + x + 7 \equiv 0 \pmod{7^3}$.
Las soluciones de $f(x) \equiv 0 \pmod 7$ son $x \equiv 0, -1 \pmod 7$ Además, $f'(0) = 1$, $f'(-1) = -1$. Existirá precisamente una $x^{(1)}$ correspondiente a $x_1^{(1)} = 0$ y una $x_s^{(2)}$ correspondiente a $x_1^{(2)} = -1$. Ahora (2.5) se transforma en

$$v_{s-1} \equiv -\frac{1}{7^{s-1}} f(x_{s-1}^{(1)}) \pmod 7 \qquad \text{correspondiente a } x_1^{(1)} = 0$$

$$v_{s-1} \equiv \frac{1}{7^{s-1}} f(x_{s-1}^{(2)}) \pmod 7 \qquad \text{correspondiente a } x_1^{(2)} = -1.$$

Entonces se encuentra

$$x_1^{(1)} = 0, \quad f(x_1^{(1)}) = 7, \quad v_1 = -1, \quad x_2^{(1)} = -7, \quad f(x_2^{(1)}) = 49,$$
$$v_2 = -1, \quad x_3^{(1)} = -56,$$
$$x_1^{(2)} = -1, \quad f(x_1^{(2)}) = 7, \quad v_1 = 1, \quad x_2^{(2)} = 6, \quad f(x_2^{(2)}) = 49,$$
$$v_2 = 1, \quad x_3^{(2)} = 55.$$

Las soluciones de $x^2 + x + 7 \equiv 0 \pmod{7^3}$ son $x \equiv -56 \pmod{7^3}$ y $x \equiv 55 \pmod{7^3}$.

Cuando se resuelven problemas numéricos, con frecuencia debe determinarse si un entero $k$ divide o no a otro entero $n$. Si $(k, 10) = 1$ y $k$ no es demasiado grande, existe un método sencillo para hacerlo. Como un primer ejemplo considérese $k = 31$, $n = 23754$. Entonces $n - 4k = 23754 - 4 \cdot 30 - 4 = 10(2375 - 4 \cdot 3) = 10 \cdot 2363$. Dado que $(31, 10) = 1$ se ve que $31 | 23754$ si y solamente si $31 | 2363$. Puede repetirse el argumento hasta reducir 2363 todavía más. El proceso completo puede ponerse en una forma más conveniente

```
 23754
    12
 -----
  2363
     9
  ----
   227
   21
   ---
     1        31 ∤ 23754.
```

Este proceso puede aplicarse para cualquier $k$ cuyo último dígito sea 1. Puede escribirse $k = 10j + 1$ y $n = 10a + b$. Entonces $n - bk = 10a + b - 10bj - b = 10(a - bj)$ y $k|n$ si y solamente si $k|(a - bj)$.

Si el último dígito de $k$ es 9, puede escribirse $k = 10j - 1$ y $n = 10a$ + b y se tiene $n + bk = 10a + b + 10bj - b = 10(a + bj)$. Entonces $k|n$ si y solamente si $k|(a + bj)$. Si el último dígito de $k$ es 3, puede escribirse $3k = 10j - 1$ y encontrar $n + 3bk = 10(a + bj)$ y de aquí que $k|n$ si y solamente si $k|(a + bj)$. De modo semejante, si el último dígito de $k$ es 7, se escribe $3k = 10j + 1$ y se obtiene $k|n$ si y solamente si $k|(a - bj)$.

**Ejemplo.**

```
19 = 10 · 2 − 1          3 · 7 = 10 · 2 + 1
20513                    8638
    6                      16
-----                    ----
2057                     847
  14                     14
----                     ---
219                      70
18
---
39
19 ∤ 20513               7|8638
```

**Problemas**

1. El método anterior determina si $k$ divide a $n$, pero en general el número que se obtiene finalmente no es congruente a $n$ módulo $k$. Considérese el siguiente esquema, ejemplificado para $n = 1234$.

```
    1 2 3 4
    3 6 9
  1 0 8
  3 0
  9
```

Aquí se ha escrito 1234 y a continuación, sucesivamente $3 \cdot 123$, $3 \cdot 36$, $3 \cdot 10$, $3 \cdot 3$. En cada paso se eliminó el dígito de la derecha y lo que quedó se multiplicó por 3. Ahora bien, se tiene $n = 1234 \equiv 4 + 9 + 8 + 0 + 9 \equiv 30 \equiv 2 \pmod 7$ y también $n = 1234 \equiv 4 - 9 + 8 - 0 + 9 \equiv 12 \pmod{13}$. Demostrar por qué puede seguirse este procedimiento para todo entero positivo $n$. ¿Qué multiplicador debe usarse en lugar de 3 si el módulo $k$ es 9 o bien 11; si $k = 17$; si $k = 19$?

Para $k = 17$ y 19 el procedimiento probablemente sea demasiado largo para tener importancia práctica. Encontrar variaciones del método que sean más satisfactorias. Por ejemplo:

```
        1 7 3 4 5 6 2
        8 6 7 2 5
      4 3 3 5
    2 1 5
  1 0
```

$1734562 \equiv 62 + 25 + 35 + 15 + 10 \equiv 147 \equiv 47 + 5 \equiv 52$
$\equiv 14 \pmod{19}$.

2. Demostrar que para $k = 9$, el método del texto y el método del problema 1 son esencialmente iguales y que equivalen al conocido proceso de "eliminación de los nueves".
3. Haciendo uso del hecho de que $1001 = 7 \cdot 11 \cdot 13$ y suponiendo que el lector puede reconocer todos los múltiplos de 7 o bien 11 o bien 13 que no tengan más de tres dígitos, diseñar un esquema para hacer la prueba de la divisibilidad entre 7 o bien 11 o bien 13, simultáneamente.
4. Probar que $(y - vp^{s-1})^j \equiv y^j + jy^{j-1}vp^{s-1} \pmod{p^s}$ si $s \geqq 2$. Probar que

$$f(y + vp^{s-1}) - f(y) \equiv \sum_{i=0}^{n-1} (n - i)a_i y^{n-i-1} vp^{s-1} \pmod{p^s} \text{ si } s \geqq 2$$

y $f(x) = \sum_{i=0}^{n} a_i x^{n-i}$.

Esto puede usarse para reemplazar el uso del desarrollo de Taylor al principio de esta sección.

5. Aplicar el método de esta sección para resolver $ax - 1 \equiv 0 \pmod{p^s}$, $(a, p) = 1$ ¿Cómo pueden relacionarse estas soluciones a las dadas por el Problema 11 de la sección 2.3 con $m$ reemplazado por $p^s$?
6. Resolver $x^5 + x^4 + 1 \equiv 0 \pmod{3^4}$.
7. Resolver $x^3 + x + 57 \equiv 0 \pmod{3^3}$.
8. Resolver $x^2 + 5x + 24 \equiv 0 \pmod{36}$.
9. Resolver $x^3 + 10x^2 + x + 3 \equiv 0 \pmod{3^3}$.
10. Resolver $x^3 + x^2 - 4 \equiv 0 \pmod{7^3}$.
11. Resolver $x^3 + x^2 - 5 \equiv 0 \pmod{7^3}$.

## 2.7 Módulo primo

Ahora se ha reducido el problema de resolver $f(x) \equiv 0 \pmod{m}$ a su último paso, congruencias con módulos primos. Es aquí en donde no será posible encontrar un método general. Sin embargo, existen algunos hechos generales referentes a las soluciones y se encontrará que conducen a algunos temas nuevos e interesantes.

Como antes, escribimos $f(x) = a_0x^n + a_1x^{n-1} + \cdot \cdot \cdot + a_n$ y suponemos que $p$ es primo y $a_0 \not\equiv 0 \pmod{p}$.

**Teorema 2.19** *Si el grado n de* $f(x) \equiv 0 \pmod{p}$ *es mayor que o igual a p, entonces todo entero es solución de* $f(x) \equiv 0 \pmod{p}$ *o bien existe un polinomio* $g(x)$ *con coeficientes enteros, cuyo coeficiente inicial es* 1 *y tal que* $g(x) \equiv 0 \pmod{p}$ *es de grado menor que p y las soluciones de* $g(x) \equiv 0 \pmod{p}$ *son precisamente las de* $f(x) \equiv 0 \pmod{p}$.

*Demostración.* Dividiendo $f(x)$ entre $x^p - x$ se obtiene $f(x) = q(x)(x^p - x) + r(x)$, donde $q(x)$ es un polinomio con coeficientes enteros y $r(x)$ es cero o un polinomio con coeficientes enteros y grado menor que $p$. El teorema de Fermat demuestra que $u^p - u \equiv 0 \pmod{p}$ y de aquí que $f(u) \equiv r(u) \pmod{p}$ para todo entero $u$. Por lo tanto, si $r(x)$ es cero o si todo coeficiente en $r(x)$ es divisible entre $p$, entonces todo entero es una solución de $f(x) \equiv 0 \pmod{p}$. La única otra posibilidad es que $r(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m$, $m < p$, $(b_0, p) = 1$. En este caso existe un entero $b$ tal que $bb_0 \equiv 1 \pmod{p}$ y, evidentemente, $r(x) \equiv 0 \pmod{p}$ y $br(x) \equiv 0 \pmod{p}$ tienen las mismas soluciones. Solamente es necesario tomar $g(x) = br(x)$.

En el enunciado del Teorema 2.19, $g(x)$ se describe con la propiedad de que $g(x) \equiv 0 \pmod{p}$ y $f(x) \equiv 0 \pmod{p}$ tienen las mismas soluciones. Con base en la demostración del teorema se ve que $g(u) \equiv bf(u) \pmod{p}$ para todo entero $u$. Sin embargo, no se dice que los polinomios $g(x)$ y $bf(x)$ sean congruentes módulo $p$; usaremos esta última proposición para dar a entender que cada coeficiente en $g(x)$ es congruente módulo $p$ al coeficiente correspondiente en $bf(x)$.

**Teorema 2.20** *La congruencia* $f(x) \equiv 0 \pmod{p}$ *de grado n tiene cuando más n soluciones.*

*Demostración.* La demostración es por inducción sobre el grado de $f(x) \equiv 0 \pmod{p}$. Si $n = 0$, el polinomio es precisamente $a_0$ con $a_0 \not\equiv 0 \pmod{p}$ y de aquí que la congruencia no tiene solución. Si $n = 1$, la congruencia tiene exactamente una solución, de acuerdo con el Teorema 2.13. Suponiendo la veracidad del teorema para todas las congruencias de grado $< n$, supóngase que existen más de $n$ soluciones de la congruencia $f(x) \equiv 0 \pmod{p}$ de grado n. Sea $a_0x^n$ el primer término de $f(x)$ y sean $u_1, u_2, \ldots, u_n, u_{n+1}$ las soluciones de la congruencia, con $u_i \not\equiv u_j \pmod{p}$ para $i \neq j$. Defínase $g(x)$ por la ecuación.

$$g(x) = f(x) - a_0(x - u_1)(x - u_2)\cdots(x - u_n),$$

notando la cancelación de $a_0x^n$ a la derecha. Entonces $g(x)$ es idénticamente cero o bien es un polinomio de grado $k$, $0 \leqq k < n$.

Se desea probar que $g(x)$ es idénticamente cero o bien es un polinomio que tiene todos sus coeficientes divisibles entre $p$. Si no fuera

así, la congruencia $g(x) \equiv 0 \pmod p$ tendría un grado, digamos $k$, y se ve que $k < n$. Pero $g(x) \equiv 0 \pmod p$ tiene $n$ soluciones $u_1$, $u_2, \ldots, u_n$, y, con base en hipótesis de inducción, es imposible.

Ahora bien, lo que se ha probado acerca de $g(x)$ demuestra que $g(u) \equiv 0 \pmod p$ para todos los enteros $u$ y de aquí que $f(u) \equiv a_0(u - u_1)(u - u_2) \cdots (u - u_n) \pmod p$ para todos los enteros $u$. En particular, $a_0(u_{n+1} - u_1)(u_{n+1} - u_2) \cdots (u_{n+1} - u_n) \equiv f(u_{n+1}) \equiv 0$ (mod p). Pero esto contradice al Teorema 1.15 y de aquí que la suposición de que $f(x) \equiv 0 \pmod p$ tiene más de $n$ soluciones es falsa.

**Corolario 2.21** *Si* $b_0x^n + b_1x^{n-1} + \cdots b_n \equiv 0 \pmod p$ *tiene más de* $n$ *soluciones entonces todos los coeficientes* $b_j$ *son divisibles entre* $p$.

**Teorema 2.22** *La congruencia* $f(x) \equiv 0 \pmod p$ *de grado* $n$, *con coeficiente inicial* $a_0 = 1$, *tiene* $n$ *soluciones si y solamente si* $f(x)$ *es un factor de* $x^p - x$ *módulo* $p$, *esto es, si y solamente si* $x^p - x = f(x)q(x) + ps(x)$ *donde* $q(x)$ *y* $s(x)$ *tienen coeficientes enteros y donde* $s(x)$ *es un polinomio de grado menor que* $n$ *o bien* $s(x)$ *es cero.*

*Demostración.* Si $f(x) \equiv 0 \pmod p$ tienen $n$ soluciones, entonces $n \leqq p$. Dividiendo $x^p - x$ entre $f(x)$ se encuentra $x^p - x = f(x)q(x) + r(x)$ donde $r(x)$ es cero o bien tiene un grado menor que $n$. Para toda solución $u$ de $f(x) \equiv 0 \pmod p$ se tiene $u^p - u \equiv 0 \pmod p$ y de aquí que $r(u) \equiv 0 \pmod p$. Por tanto, si $r(x)$ no es cero, es un polinomio de grado menor que $n$ teniendo $n$ soluciones. De acuerdo con el Corolario 2.21, todos los coeficientes de $r(x)$ son divisibles entre $p$ y puede escribirse $r(x) = ps(x)$.

Inversamente, si $x^p - x = f(x)q(x) + ps(x)$, entonces $f(u)q(u) \equiv u^p - u - ps(u) \equiv 0 \pmod p$ para todo entero $u$. Por lo tanto, $f(x)q(x) \equiv 0 \pmod p$ tiene $p$ soluciones. Pero $q(x)$ es de grado $p - n$ y de aquí que tiene cuando más $p - n$ soluciones, $v_1, v_2, \ldots, v_k$, digamos, con $k \leqq p - n$. Si $u$ es cualquiera de los otros $p - k$ residuos módulo $p$, entonces $(q(u), p) = 1$ y $f(u)q(u) \equiv 0 \pmod p$ y, por el Teorema 1.9, se tiene $f(u) \equiv 0 \pmod p$. De aquí que $f(x) \equiv 0 \pmod p$ tiene por lo menos $p - k \geqq p - (p - n) = n$ soluciones. Esto, con el Teorema 2.20, demuestra que $f(x) \equiv 0 \pmod p$ tiene exactamente $n$ soluciones.

La restricción $a_0 = 1$ en este teorema es necesaria para que pueda dividirse $x^p - x$ entre $f(x)$ y obtener un polinomio $q(x)$ con coeficientes enteros. Sin embargo, no es una gran restricción. Siempre es posible encontrar un entero $a$ tal que $aa_0 \equiv 1 \pmod p$. Entonces $af(x) - (aa_0 - 1)x^n \equiv 0 \pmod p$ tiene las mismas soluciones que $f(x) \equiv 0 \pmod p$ y $af(x) - (aa_0 - 1)x^n$ tiene a 1 como coeficiente inicial.

**Problemas**

1. Reducir las siguientes congruencias a congruencias equivalentes de grado $\leqq 6$:
   *a*) $x^{11} + x^8 + 5 \equiv 0 \pmod 7$;
   *b*) $x^{20} + x^{13} + x^7 + x \equiv 2 \pmod 7$;
   *c*) $x^{15} - x^{10} + 4x - 3 \equiv 0 \pmod 7$.
2. Probar, mediante la aplicación del Teorema 2.22, que $2x^3 + 5x^2 + 6x + 1 \equiv 0 \pmod 7$ tiene tres soluciones.
3. Probar que $x^{14} + 12x^2 \equiv 0 \pmod{13}$ tiene 13 soluciones y, por lo tanto, que es una congruencia idéntica.
4. Probar que si $f(x) \equiv 0 \pmod p$ tiene $j$ soluciones $x \equiv a_1$, $x \equiv a_2$, $\ldots, x \equiv a_j \pmod p$, existe un polinomio $q(x)$ tal que $f(x) \equiv (x - a_1)(x - a_2) \cdots (x - a_j)q(x) \pmod p$. *Sugerencia*: empezar por demostrar que existe un $q_1(x)$ tal que $f(x) \equiv (x - a_1)q_1(x) \pmod p$ y que $q_1(x) \equiv 0 \pmod p$ tiene las soluciones $x \equiv a_2$, $x \equiv a_3$, $\ldots$, $x \equiv a_j \pmod p$. Entonces aplicar la inducción.
5. Con las suposiciones y la notación del problema anterior, probar que si el grado de $f(x)$ es $j$, entonces $q(x)$ es una constante y puede tomarse como el coeficiente inicial de $f(x)$.
6. Probar que el teorema de Fermat implica que

$$x^p - 1 \equiv (x - 1)(x - 2) \cdots (x - p + 1) \pmod p$$

y $$x^p - x \equiv x(x - 1)(x - 2) \ldots (x - p + 1) \pmod p.$$

7. Por comparación de los coeficientes de $x$ en el problema anterior, dar otra demostración del teorema de Wilson.
8. Sea $m$ compuesto. Probar que el Teorema 2.20 es falso si "mod $p$" se reemplaza por "mod $m$".

## 2.8 Congruencias de grado dos, módulo primo

Si $f(x) \equiv 0 \pmod p$ es de grado dos, entonces $f(x) = ax^2 + bx + c$ y $a$ es relativamente primo para $p$. Se supondrá que $p > 2$ dado que el caso $p = 2$ no presenta dificultades. Entonces $p$ es impar y $4af(x) = (2ax + b)^2 + 4ac - b^2$. De aquí que $u$ es una solución de $f(x) \equiv 0 \pmod p$ si y solamente si $2au + b \equiv v \pmod p$, donde $v$ es una solución de $v^2 \equiv b^2 - 4ac \pmod p$. Además, supuesto que $(2a, p) = 1$, para cada solución $v$ existe uno, y solamente un, $u$ módulo $p$ tal que $2au + b \equiv v \pmod p$. Evidentemente, diferente $v$ módulo $p$ proporciona diferente $u$ módulo $p$. De modo que el problema de resolver la congruencia de grado dos se reduce a la de resolver una congruencia de la forma $x^2 \equiv a \pmod p$.

En el capítulo 3 se considerará con todo detalle la congruencia $x^2 \equiv a$ (mod p). Por el momento simplemente obtendremos algunos resultados generales referentes a la congruencia más general $x^n \equiv a \pmod p$ y ciertos conceptos relacionados con el tema.

**Problema**

1. Reducir las siguientes congruencias a la forma $x^2 \equiv a \pmod{p}$:

a) $4x^2 + 2x + 1 \equiv 0 \pmod{5}$; c) $2x^2 + 7x - 10 \equiv 0 \pmod{11}$;
b) $3x^2 - x + 5 \equiv 0 \pmod{7}$; d) $x^2 + x - 1 \equiv 0 \pmod{13}$.

## 2.9. Residuos de potencias

**Definición 2.6** *Si $x^n \equiv a \pmod{p}$ tiene una solución, entonces a recibe el nombre de $n$-ésimo residuo de potencia módulo p.*

**Definición 2.7** *Sea m un entero positivo y a cualquier entero tal que $(a, m) = 1$. Sea h el menor entero positivo tal que $a^h \equiv 1 \pmod{m}$. Se dice que a pertenece al exponente h módulo m.*

Puesto que, por el teorema de Euler, $a^{\phi(m)} \equiv 1 \pmod{m}$, se ve que todo $a$ relativamente primo para $m$, pertenece al algún exponente $h \leqq \phi(m)$ módulo $m$. Dividiendo $\phi(m)$ entre $h$ se obtiene $\phi(m) = qh + r$, $0 \leqq r < h$. Pero entonces $a^r \equiv a^{r+qh} \equiv a^{\phi(m)} \equiv 1 \pmod{m}$. Supuesto que $h$ es el menor entero positivo tal que $a^h \equiv 1 \pmod{m}$ y dado que $0 \leqq r < h$, se ve que $r$ no puede ser positivo. Por lo tanto, $r = 0$ y se tiene la primera aseveración del siguiente teorema.

**Teorema 2.23** *Si a pertenece al exponente h módulo m, entonces $h|\phi(m)$. Además, $a^j \equiv a^k \pmod{m}$ si y solamente si $h|(j - k)$.*

*Demostración.* No se pierde generalidad suponiendo $j > k$ y, dado que $(a, m) = 1$, la congruencia $a^j \equiv a^k \pmod{m}$ es equivalente a $a^{j-k} \equiv 1 \pmod{m}$. De donde se deduce la segunda aseveración del teorema como en la demostración de la primera.

**Teorema 2.24** *Si a pertenece al exponente h módulo m, entonces $a^k$ pertenece al exponente $h/(h, k)$ módulo m.*

*Demostración.* De acuerdo con el Teorema 2.23, $(a^k)^j \equiv 1 \pmod{m}$ si y solamente si $h|kj$. Pero $h|kj$ si y solamente si $\{h/(h,k)\}|\{k/(h, k)\}j$ y de aquí que si y solamente si $\{h/(h, k)\}|j$. Por tanto, el menor entero positivo $j$ tal que $(a^k)^j \equiv 1 \pmod{m}$ es $j = h/(h, k)$.

**Definición 2.8** *Si a pertenece al exponente $\phi(m)$ módulo m, entonces a recibe el nombre de raíz primitiva módulo m.*

**Teorema 2.25** *Si p es primo, entonces existen $\phi(p - 1)$ raíces primitivas módulo p. Los únicos enteros que tienen raíces primitivas son $p^e$, $2p^e$, 2 y 4, con p primo impar.*

*Demostración.* Cada entero $a$, $1 \leqq a \leqq p - 1$, pertenece a algún exponente $h$, módulo $p$ con $h|(p - 1)$. Si $a$ pertenece al exponente $h$,

entonces $(a^k)^h \equiv 1 \pmod{p}$ para todo $k$, y $1, a, a^2, \ldots; a^{h-1}$ son distintos módulo $p$. Por tanto, con base en el Teorema 2.20, estos números $h$ son todos las soluciones de $x^h \equiv 1 \pmod{p}$. Por el Teorema 2.24, precisamente $\phi(h)$ de estos números pertenecen al exponente $h$ módulo $p$. Los demás pertenecen a exponentes menores. También, cualquier entero $a$ que pertenece el exponente $h$ módulo $p$ es una solución de $x^h \equiv 1 \pmod{p}$. Por lo tanto, para cada $h$ que divide a $p-1$, existirán $\phi(h)$ enteros $a$ o ninguno, $1 \leqq a \leqq p-1$, tales que $a$ pertenece al exponente $h$ módulo $p$. Denotemos por $\psi(h)$ el número de los enteros $a$ que pertencen al exponente $h$ módulo $p$. Entonces $\psi(h) \leqq \phi(h)$ para cada $h$ que divide a $p-1$ y $\sum_{h|p-1} \psi(h) = p-1$. Pero $\sum_{h|p-1} \phi(h) = p - 1$, de acuerdo con el Teorema 2.17, de modo que se tiene $\sum_{h|p-1} (\psi(h) - \phi(h)) = 0$ y $\psi(h) - \phi(h) \leqq 0$. Esto implica que $\psi(h) = \phi(h)$ para todo $h$ que divide a $p-1$ y, en particular, $\psi(p-1) = \phi(p-1) > 0$. Esto demuestra que la primera parte del teorema es cierta.

Fácilmente se ve que $\phi(n)$ es par para $n > 2$. Sea $m = 2^f \prod_{i=1}^{k} p_i^{e_i}$, donde los $p_i$ son primos impares distintos, $f \geqq 0$, $e_i > 0$ y $k \geqq 1$. Si $(a, m) = 1$. se tiene $a^{\phi(p_i e_i)} \equiv 1 \pmod{p_1^{e_1}}$ y $a^{\phi(m/p_1 e_1)} \equiv 1 \pmod{m/p_1^{e_1}}$. Supóngase que $k \geqq 2$ o bien $f \geqq 2$. Entonces tanto $\phi(p_1^{e_1})$ como $\phi(m/p_1^{e_1})$ son pares y por tanto $a^{\frac{1}{2}\phi(p_1 e_1)\phi(m/p_1 e_1)}$ es congruente a 1 módulo $p_1^{e_1}$ y módulo $m/p_1^{e_1}$, de aquí módulo $m$. Esto demuestra que los únicos $m$ que posiblemente pueden tener raíces primitivas son $p^e$, $2p^e$, 2 y 4, con $p$ primo impar.

Considérese $m = p^e$ y sea $a$ una raíz primitiva módulo $p$. Sea $b = a + pt$. Entonces, por el teorema del binomio,

$$b^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}pt \pmod{p^2}$$

y puede escogerse $t$ para hacer $b^{p-1} = 1 + n_1 p$ con $n_1 \not\equiv 0 \pmod{p}$. Observando que $(1 + np^{j-1})^p \equiv 1 + np^j$ (mod $p^{2j-1}$ se aplica la inducción para ver que $b^{p^{j-1}(p-1)} = 1 + n_j p^j$ con $n_j \equiv n_{j-1} \pmod{p^{j-1}}$. Entonces $n_j \equiv n_1 \not\equiv 0 \pmod{p}$. Supóngase que $b$ pertenece al exponente $h$ módulo $p^e$, para $e \geqq 2$. Entonces $h | p^{e-1}(p-1)$ y de aquí que $h = p^s d$, $s \leqq e - 1$, lo cual implica $b^{p^s(p-1)} \equiv 1 \pmod{p^e}$, $1 + n_{s+1}p^{s+1} \equiv 1 \pmod{p^e}$ y, por lo tanto $s \geqq e-1$, $s = e-1$. También se tiene $b^d \equiv b^{p^s d} \equiv 1 \pmod{p}$ lo cual implica que $(p-1)|d$, por el Teorema 2.23, dado que $b \equiv a \pmod{p}$ y $a$ pertenece al exponente $p-1$. Entonces se tiene $h = \phi(p^e)$ y $b$ es una raíz primitiva módulo $p^e$. Obsérvese que $b$ es independiente de $e$.

Ahora considérese $m \equiv 2p^e$ y sea $a$ una raíz primitiva módulo $p^e$. Sea $b = a$ o bien $a + p^e$, el cual es impar. Entonces $b^h \equiv 1 \pmod{2}$ para

todo $h$ y $b^h \equiv a^h \equiv 1 \pmod{p^e}$ si y solamente si $p^{e-1}(p-1) \mid h$. Esto implica que $b$ es una raíz primitiva módulo $2p^e$.

Finalmente, obsérvese que 3 es una raíz primitiva módulo 4.

**Teorema 2.26** *Supóngase que $m$ tiene una raíz primitiva $g$. Entonces $g^j \equiv g^k \pmod{m}$ si y solamente si $j \equiv k \pmod{\phi(m)}$; en particular, $g^j \equiv 1 \pmod{m}$ si y solamente si $\phi(m) \mid j$. El conjunto $g, g^2, \ldots, g^{\phi(m)}$ forma un sistema reducido de residuos módulo $m$, de modo que si $a$ es cualquier entero que satisface $(a, m) = 1$, existe uno y solamente un $g^j$ en el conjunto tal que $g^j \equiv a \pmod{m}$.*

*Demostración.* La primera parte del teorema es un caso especial del Teorema 2.23. Se concluye que $g, g^2, \ldots, g^{\phi(m)}$ son incongruentes en pares módulo $m$ y, por tanto, este conjunto forma un sistema reducido de residuos módulo $m$.

El exponente $j$ tal que $g^j \equiv a \pmod{m}$ se llama el *índice* de $a$. El índice depende de $m$ y $g$ así como de $a$. Los índices se comportan de modo muy semejante a los logaritmos y, en ocasiones, son útiles como auxiliares para los cálculos, además de su propio interés teórico.

**Teorema 2.27** *Si $p$ es primo y $(a, p) = 1$, entonces la congruencia $x^n \equiv a \pmod{p}$ tiene $(n, p-1)$ soluciones o bien ninguna solución, de acuerdo con que*

$$a^{(p-1)/(n,p=1)} \equiv 1 \pmod{p} \quad \text{o bien} \quad a^{(p-1)/(n,p-1)} \not\equiv 1 \pmod{p}$$

*Demostración.* Denotemos por $b$ a $(n, p-1)$. Si $x^n \equiv a \pmod{p}$ tiene una solución $u$, entonces

$$a^{(p-1)/b} \equiv u^{n(p-1)/b} \equiv u^{(p-1)(n/b)} \equiv 1 \pmod{p}.$$

Por lo tanto, $x^n \equiv a \pmod{p}$ no tiene solución si $a^{(p-1)/b} \equiv 1 \pmod{p}$.

Inversamente, supóngase que $a^{(p-1)/b} \equiv 1 \pmod{p}$. De acuerdo con los Teoremas 2.25 y 2.26, existe una raíz primitiva $g$ módulo $p$ y un exponente $j$ tal que $g^j \equiv a \pmod{p}$. Así que se tiene

$$g^{j(p-1)/b} \equiv a^{(p-1)/b} \equiv 1 \pmod{p}$$

y esto implica que $j(p-1)/b \equiv 0 \pmod{p-1}$, por el Teorema 2.26, de modo que $b \mid j$. Ahora bien, cualquier solución de $x^n \equiv a \pmod{p}$, si existe, también puede escribirse como una potencia de $g$, digamos $g^y$, módulo $p$. De aquí que las soluciones en $x$, si existen, de $x^n \equiv a \pmod{p}$ corresponden a las soluciones en $y$ de $g^{yn} \equiv g^j \pmod{p}$. Esta congruencia, de acuerdo con el Teorema 2.23, tiene soluciones si y solamente si $yn \equiv j \pmod{p-1}$ tiene soluciones, la cual, por el Teorema 2.13, tiene soluciones puesto que $b \mid j$. Además, con base en el Teorema 2.13, existen $(n, p-1)$ soluciones y así se tienen $(n, p-1)$ soluciones de $x^n \equiv a \pmod{p}$.

**Corolario 2.28** *Si $p$ es un primo impar y $(a, p) = 1$, entonces $x^2 \equiv a \pmod{p}$ tiene dos soluciones o ninguna de acuerdo con que $a^{(p-1)/2} \equiv 1$ o bien $-1 \pmod{p}$.*

*Demostración.* A partir del teorema de Fermat se tiene

$$(a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1) \equiv a^{p-1} - 1 \equiv 0 \pmod{p}$$

y de aquí que $a^{(p-1)/2} \equiv \pm 1 \pmod{p}$.

**Problemas**

1. Encontrar una raíz primitiva del primo 3, del primo 5, del primo 7, del primo 11, del primo 13.
2. Encontrar una raíz primitiva de 23.
3. ¿Cuántas raíces primitivas tiene el primo 13?
4. ¿Para cuáles exponentes 1, 2, 3, 4, 5 y 6, respectivamente, pertenecen al módulo 7?
   ¿Para qué exponentes pertenecen al módulo 11?
5. Sea $p$ un primo impar. Probar que $a$ pertenece al exponente 2 módulo $p$ si y solamente si $a \equiv -1 \pmod{p}$.
6. Si $a$ pertenece al exponente $h$ módulo $m$, probar que ningún par de $a$, $a^2$, $a^3, \ldots, a^h$ son congruentes módulo $m$.
7. Si $p$ es un primo impar ¿cuántas soluciones existen para $x^{p-1} \equiv 1 \pmod{p}$? ¿para $x^{p-1} \equiv 2 \pmod{p}$?
8. Probar que 3 es una raíz primitiva de 17, observando que las potencias de 3 son congruentes a 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1 módulo 17. Entonces aplicar el Teorema 2.27 para determinar cuántas soluciones tienen cada una de las siguientes congruencias:

   (*a*) $x^{12} \equiv 16 \pmod{17}$ (*b*) $x^{48} \equiv 9 \pmod{17}$
   (*c*) $x^{20} \equiv 13 \pmod{17}$ (*d*) $x^{11} \equiv 9 \pmod{17}$

   *Sugerencia*: $16 \equiv 3^8$, $13 \equiv 3^4 \pmod{17}$.
9. Usando los datos del problema anterior, determinar cuáles de las siguientes congruencias tienen soluciones: $x^2 \equiv 1$, $x^2 \equiv 2$, $x^2 \equiv 3, \ldots, x^2 \equiv 16 \pmod{17}$.
10. Probar que si $p$ es primo y $(a, p) = 1$ y $(n, p-1) = 1$, entonces $x^n \equiv a \pmod{p}$ tiene exactamente una solución.
11. Probar que si $g$ es una raíz primitiva módulo $p$ y si $(k, p-1) = 1$, entonces $g^k$ también es una raíz primitiva.
12. Probar que si $a$ pertenece al exponente 3 módulo $p$, entonces $1 + a + a^2 \equiv 0 \pmod{p}$ y $1 + a$ pertenece al exponente 6.
13. Probar que si $a$ pertenece al exponente $h$ módulo primo $p$ y si $h$ es par, entonces $a^{h/2} \equiv -1 \pmod{p}$.
14. Probar que si $a$ pertenece a un exponente $h$ y $b$ a un exponente $k$, módulo $m$, entonces $ab$ pertenece a un exponente el cual es un divisor de $hk$. Además, si $(h, k) = 1$, entonces $ab$ pertenece al exponente $hk$ módulo $m$. *Sugerencia*: si $ab$ pertenece al exponente $r$, entonces

$$1 \equiv (ab)^r \equiv (ab)^{hr} \equiv (a^h)^r b^{hr} \equiv b^{hr} \pmod{m},$$

   de manera que $k \mid hr$.

15. Dado que $ab \equiv 1 \pmod m$ y que $a$ pertenece al exponente $h$ módulo $m$, probar que $b$ pertenece al exponente $h$. A continuación probar que si $p > 3$, el producto de todas las raíces primitivas de $p$ es congruente a 1 módulo $p$.
16. Sean $a$ y $n > 1$ enteros cualesquiera tales que

$$a^{n-1} \equiv 1 \pmod n \text{ pero } a^x \not\equiv 1 \pmod n$$

para todo divisor propio $x$ de $n - 1$. Probar que $n$ es primo.
17. Para cualquier primo $p$ y cualquier entero $a$ tal que $(a, p) = 1$, digamos que $a$ es un residuo cúbico de $p$ si $x^3 \equiv a \pmod p$ tiene por lo menos una solución. Probar que si $p$ es de la forma $3k + 2$, entonces todos los enteros en un sistema reducido de residuos módulo $p$ son residuos cúbicos, mientras que si $p$ es de la forma $3k + 1$, solamente un tercio de los miembros de un sistema reducido de residuos son residuos cúbicos.
18. Probar el teorema de Wilson usando las raíces primitivas.
19. Sea $p$ un primo impar. Sean $r_1, r_2, \cdots, r_{p-1}$ los enteros $1, 2, \cdots, p - 1$ en cualquier orden. Probar que por lo menos dos de los números $1 \cdot r_1, 2 \cdot r_2, \ldots, (p-1)r_{p-1}$ son congruentes módulo $p$.

Los siguientes problemas constituyen un conjunto relacionado:

20. Considérese el desarrollo decimal infinito $\alpha = .\alpha_1\alpha_2\alpha_3 \cdots$ para la base diez, donde la sucesión de dígitos no son todos ceros ni todos nueves más allá de cierto punto. De modo semejante, sea $\beta = .\beta_1\beta_2\beta_3 \cdots$. Probar que $\alpha = \beta$ si y solamente si $\alpha_j = \beta_j$, para todo $j = 1, 2, 3, \ldots$.
21. Se dice que el desarrollo decimal de $\alpha$ es periódico si existe un entero positivo $k$ y un entero $n_0$ no negativo tales que $\alpha_{n+k} = \alpha_n$ para todos los enteros $n > n_0$. Si el desarrollo decimal de $\alpha$ es periódico, el menor entero $k$ que llena el requisito antes mencionado se llama período de $\alpha$. Si $n_0 = 0$, entonces el desarrollo decimal de $\alpha$ se dice que es puramente periódico. Probar que un número real es racional si y solamente si su desarrollo decimal es finito (termina) o bien es periódico.
22. Sean $a$ y $b$ enteros positivos con $a < b$ y $(a, b) = 1$. Probar que el desarrollo decimal de $a/b$ termina o tiene una sucesión infinita de nueves si y solamente si los únicos primos que dividen a $b$ son 2 y 5. Probar que el desarrollo decimal de $a/b$ es puramente periódico si y solamente si $b$ no es divisible entre 2 ni entre 5.
23. Suponiendo que $(b, 10) = 1$, sea $k$ la potencia de 10 a la cual pertenece $b$. Probar que $k$ es el período del desarrollo decimal de $a/b$. *Sugerencia*: $(10^k - 1)a/b$ es un entero.
24. Suponiendo que $(b, 10) > 1$, escribir $b = 2^r5^sb_0$ donde $(b_0, 10) = 1$. Supóngase que $b_0 > 1$ y sea $k_0$ la potencia de 10 a la cual pertenece $k_0$. Escribir $t = \text{máx }(r, s)$. Probar que el período del desarrollo decimal de $a/b$ es $k_0$ y que la longitud del bloque de dígitos no periódico (es decir, el menor valor de $n_0$ aplicable en la definición dada anteriormente) es $t$.

## 2.10 Teoría de los números desde un punto de vista algebraico

En esta sección y en la siguiente discutiremos algunas de las formas en las cuales los conceptos elementales de la teoría de los números surgen en el álgebra. La teoría de los números proporciona una fuente

rica de ejemplos de las estructuras del álgebra abstracta. Trataremos brevemente tres de estas estructuras: grupos, anillos y campos.

Antes de dar la definición técnica de grupo, expliquemos algo del lenguaje usado, las operaciones como la adición y la multiplicación se llaman "operaciones binarias" debido a que los elementos se suman o se multiplican para producir un tercer elemento. La sustracción de pares de elementos, $a - b$, también es una operación binaria. Así como la exponenciación, $a^b$, en la cual el elemento $a$ se eleva a la $b$-ésima potencia. Ahora bien, un grupo consiste de un conjunto de elementos junto con una operación binaria sobre esos elementos, tales que se cumplen ciertas propiedades. Los grupos teóricos de números con los cuales trabajaremos tendrán enteros o bien conjuntos de enteros como elementos y la operación será la adición o bien la multiplicación. Sin embargo, un grupo general puede tener elementos de cualquier tipo y cualquier clase de operación binaria, siempre y cuando satisfaga las condiciones que impondremos dentro de algunos párrafos.

Empecemos con una operación binaria general denotada por $\oplus$ y supondremos que esta operación binaria es unívoca. Esto significa que para cada $a$, $b$ de elementos, $a \oplus b$ tiene un valor único y o bien no está definido. Se dice que un conjunto de elementos es "cerrado" respecto a una operación $\oplus$, o bien es cerrado "bajo" la operación, si $a \oplus b$ está definido y es un elemento del conjunto para todo par de elementos $a$, $b$ del conjunto. Por ejemplo, los números naturales 1, 2, 3, . . . constituyen un conjunto cerrado bajo la adición pero no es cerrado bajo la sustracción. Se dice que un elemento $e$ es un "elemento identidad" de un conjunto respecto a la operación $\oplus$ si se cumple la propiedad

$$a \oplus e = e \oplus a = a$$

para todo elemento $a$ en el conjunto. Cuando los elementos del conjunto son números, entonces $e$ es el elemento cero, $e = 0$, si $\oplus$ es la adición ordinaria, mientras que $e$ es el elemento unidad, $e = 1$, si $\oplus$ es la multiplicación ordinaria. Suponiendo la existencia de un elemento identidad $e$, se dice que un elemento $a$ tiene un "inverso", denotado por $a^{-1}$, si se cumple la propiedad

$$a \oplus a^{-1} = a^{-1} \oplus a = e.$$

Si los elementos son números y $\oplus$ es la adición ordinaria, generalmente se escribe $a + b$ en lugar de $a \oplus b$ y $-a$ para el inverso $a^{-1}$ debido a que el inverso aditivo es el negativo del número $a$. Por otra parte, si la operación $\oplus$ es la multiplicación ordinaria, se escribe $a \cdot b$ por $a \oplus b$. En este caso, la notación $a^{-1}$ es la acostumbrada en el álgebra elemental para el inverso multiplicativo. Aquí, y en toda esta sección, la palabra "número" significa cualquier número, entero, racional, real o complejo.

**Definición 2.9** *Un grupo G es un conjunto de elementos a, b, c, . . . junto con una operación binaria unívoca* $\oplus$ *tal que*

1) *el conjunto es cerrado bajo la operación;*
2) *se cumple la ley asociativa, a saber,* $a \oplus (b \oplus c) = (a \oplus b) \oplus c$ *para todos los elementos a, b, c en G;*
3) *el conjunto tiene un elemento identidad único, e;*
4) *cada elemento en G tiene un inverso único en G.*

*Un grupo G se llama "abeliano" o "conmutativo" si* $a \oplus b = b \oplus a$ *para todo par de elementos a, b en G. Un "grupo finito" es uno con un número finito de elementos; en caso contrario es un "grupo infinito". Si un grupo es finito, el número de sus elementos recibe el nombre de "orden" del grupo.*

Las propiedades 1, 2, 3 y 4 no son los postulados mínimos posibles para un grupo. Por ejemplo, en el postulado 4 podría haberse requerido simplemente que cada elemento $a$ tenga un inverso izquierdo, esto es, un inverso $a'$ tal que $a' \oplus a = e$ y entonces probar la segunda parte del postulado 4 como una consecuencia. Sin embargo, para evitar una discusión demasiado larga de la teoría de los grupos, dejaremos esos refinamientos para los libros de álgebra.

El conjunto de todos los enteros $0, \pm 1, \pm 2, \ldots$ es un grupo bajo la adición; de hecho es un grupo abeliano. Pero los enteros no constituyen un grupo bajo la multiplicación debido a la ausencia de inversos para todos los elementos excepto $\pm 1$.

Otro ejemplo de grupo se obtiene considerando las congruencias módulo $m$. En el caso de $m = 6$, para dar un ejemplo concreto, estamos familiarizados con congruencias sencillas tales como

$$3 + 4 \equiv 1 \pmod 6, \qquad 5 + 5 \equiv 4 \pmod 6.$$

Se obtiene "el grupo aditivo módulo 6" tomando un sistema completo de residuos, digamos 0, 1, 2, 3, 4, 5 y reemplazando la congruencia módulo 6 por la igualdad

$$3 + 4 = 1, \qquad 5 + 5 = 4.$$

La tabla de adición completa para este sistema es:

| $\oplus$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 |
| 1 | 1 | 2 | 3 | 4 | 5 | 0 |
| 2 | 2 | 3 | 4 | 5 | 0 | 1 |
| 3 | 3 | 4 | 5 | 0 | 1 | 2 |
| 4 | 4 | 5 | 0 | 1 | 2 | 3 |
| 5 | 5 | 0 | 1 | 2 | 3 | 4 |

Por supuesto que podría hacerse cualquier sistema completo de residuos módulo 6; así, 1, 2, 3, 4, 5, 6, o bien 7, $-2$, 17, 30, 8, 3 podrían servir como elementos, bajo el supuesto de que se realizan adiciones módulo 6. Si se usara el sistema 7, $-2$, 17, 30, 8, 3 la tabla de adición resultaría diferente. Sin embargo, los dos grupos son esencialmente los mismos; solamente se han dado nombres nuevos a los elementos: 0 ahora se llama 30, 1 es 7, y así sucesivamente. Se dice que los dos grupos son "isomorfos" y no se considerarán los grupos isomorfos como diferentes. Así, se hablará de "el" grupo aditivo módulo 6 y no de "un" grupo aditivo módulo 6.

**Definición 2.10** *Se dice que dos grupos, $G$ con operación $\oplus$ y $G'$ con operación $\odot$ son isomorfos si existe una correspondencia biunívoca entre los elementos de $G$ y los de $G'$, tal que si $a$ en $G$ corresponde a $a'$ en $G'$ y $b$ en $G$ corresponde a $b'$ en $G'$, entonces $a \oplus b$ en $G$ corresponde a $a' \odot b'$ en $G'$.*

Otra manera de pensar en el grupo aditivo módulo 6 es en términos de las llamadas clases residuales. Pongamos dos enteros $a$ y $b$ en la misma clase residual módulo 6 si $a \equiv b \pmod 6$ y el resultado es para separar todos los enteros en seis clases residuales:

$$\begin{array}{llrrrrrrrl}
C_0: & \cdots, & -18, & -12, & -6, & 0, & 6, & 12, & 18, & \cdots \\
C_1: & \cdots, & -17, & -11, & -5, & 1, & 7, & 13, & 19, & \cdots \\
C_2: & \cdots, & -16, & -10, & -4, & 2, & 8, & 14, & 20, & \cdots \\
C_3: & \cdots, & -15, & -9, & -3, & 3, & 9, & 15, & 21, & \cdots \\
C_4: & \cdots, & -14, & -8, & -2, & 4, & 10, & 16, & 22, & \cdots \\
C_5: & \cdots, & -13, & -7, & -1, & 5, & 11, & 17, & 23, & \cdots
\end{array}$$

Si cualquier elemento de la clase $C_2$ se suma a cualquier elemento de la clase $C_3$, la suma es un elemento en la clase $C_5$, de manera que es razonable escribir $C_2 + C_3 = C_5$. De modo semejante se observa que $C_3 + C_4 = C_1$, $C_5 + C_3 = C_2$, etc. y así podría construirse una tabla de adición para estas clases. Pero la tabla de adición así construida sería simplemente una repetición de la tabla de adición de los elementos 0, 1, 2, 3, 4, 5 módulo 6. Así, las seis clases $C_0$, $C_1$, $C_2$, $C_3$, $C_4$, $C_5$ forman un grupo bajo esta adición que es isomorfo al grupo aditivo módulo 6. Este planteamiento de la clase residual del grupo aditivo módulo 6 tiene la ventaja de que la ecuación peculiar $5 + 5 = 4$ (en la cual los símbolos tienen un significado diferente al que tienen en aritmética elemental) se reemplaza por la forma más razonable $C_5 + C_5 = C_4$.

**Teorema 2.29** *Cualquier sistema completo de residuos módulo $m$ forma un grupo bajo la adición módulo $m$. Dos sistemas completos de residuos módulo $m$ constituyen grupos isomorfos bajo la adición y así se habla de "el" grupo aditivo módulo $m$.*

*Demostración.* Empecemos con el sistema completo de residuos $0, 1, 2, \ldots, m-1$ módulo $m$. Este sistema es cerrado bajo la adición módulo $m$ y la propiedad asociativa de la adición se hereda de la propiedad correspondiente para todos los enteros, esto es $a + (b + c) = (a + b) + c$ implica $a + (b + c) \equiv (a + b) + c \pmod{m}$. El elemento identidad es 0 y es único. Finalmente, el inverso aditivo de 0 es 0 y el inverso aditivo de cualquier otro elemento $a$ es $m - a$. Estos inversos son únicos.

Pasando del sistema $0, 1, \ldots, m-1$ a cualquier sistema completo de residuos $r_0, r_1, \ldots, r_{m-1}$ se prueba que todas las observaciones anteriores se cumplen reemplazando $a$ por $r_a$, $a = 0, 1, \ldots, m-1$, de modo que esencialmente se tiene el mismo grupo con nueva notación.

**Problemas**

1. ¿Cuáles de los siguientes conjuntos son grupos?
   *a*) los enteros pares bajo la adición;
   *b*) los enteros impares bajo la adición;
   *c*) los enteros bajo la sustracción;
   *d*) los enteros pares bajo la multiplicación;
   *e*) todos los enteros múltiplos de 7, bajo la adición;
   *f*) todos los números racionales bajo la adición (recuérdese que un número racional es uno de la forma $a/b$ donde $a$ y $b$ son enteros, con $b \neq 0$);
   *g*) el mismo conjunto dado en (*f*) pero bajo la multiplicación;
   *h*) el mismo conjunto dado en (*f*) con el elemento cero eliminado, bajo la multiplicación;
   *i*) todos los números racionales $a/b$ que tienen $b = 1$ o bien $b = 2$, bajo la adición;
   *j*) todos los números racionales $a/b$ que tienen $b = 1$, $b = 2$ o bien $b = 3$, bajo la adición.
2. Supóngase que $G$ tiene como elementos a los cuatro pares $(1, 1)$, $(1, -1)$, $(-, 1)$, $(-1, -1)$ y sea $(a, b) \oplus (c, d) = (ac, bd)$. Probar que $G$ es un grupo.
3. Usando el sistema completo de residuos 7, −2, 17, 30, 8, 3 escribir la tabla de adición para el grupo aditivo módulo 6. Reescribir esta tabla reemplazando 7 por 1, 30 por 0, etc. Verificar que esta tabla da los mismos valores para $a \oplus b$ que la dada en el texto.
4. Probar que el conjunto de elementos $e, a, b, c$, con la siguiente tabla para la operación binaria,

| $\oplus$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $a$ | $e$ |
| $c$ | $c$ | $b$ | $e$ | $a$ |

es un grupo. Probar que este grupo es isomorfo al grupo aditivo módulo 4.

5. Probar que el conjunto de elementos $e, u, v, w,$ con la siguiente tabla para la operación binaria,

| $\oplus$ | $e$ | $u$ | $v$ | $w$ |
|---|---|---|---|---|
| $e$ | $e$ | $u$ | $v$ | $w$ |
| $u$ | $u$ | $e$ | $w$ | $v$ |
| $v$ | $v$ | $w$ | $e$ | $u$ |
| $w$ | $w$ | $v$ | $u$ | $e$ |

es un grupo. Probar que este grupo no es isomorfo al grupo aditivo módulo 4 pero que es isomorfo al grupo descrito en el Problema 2.

6. Probar que el conjunto de elementos 1, 2, 3, 4, bajo la operación de multiplicación módulo 5, es un grupo que es isomorfo al grupo del Problema 4.
7. Probar que el conjunto de números complejos $+1, -1, +i, -i$, donde $i^2 = -1$, es un grupo bajo la multiplicación y que es isomorfo al grupo del Problema 4.
8. Probar que el isomorfismo es "transitivo", es decir, si un grupo $G_1$ es isomorfo a $G_2$, y si $G_2$ es isomorfo a $G_3$, entonces $G_1$ es isomorfo a $G_3$.
9. Probar que los elementos 1, 3, 5, 7 bajo la multiplicación módulo 8 forman un grupo que es isomorfo al grupo del Problema 5.
10. Probar que esencialmente solamente existen dos grupos de orden 4, esto es, que cualquier grupo de orden 4 es isomorfo a uno de los grupos de los Problemas 4 y 5.
11. Para cualquier entero positivo $m > 1$, separar todos los enteros en las clases $C_0, C_1, \ldots, C_{m-1}$, poniendo los enteros $r$ y $s$ en la misma clase si $r \equiv s \pmod{m}$, así que

$C_0$: $\ldots, -2m, -m, 0, m, 2m, \ldots$
$C_1$: $\ldots, -2m+1, -m+1, 1, m+1, 2m+1, \ldots$
etc.

Probar que si dos enteros cualesquiera, uno de la clase $C_a$ y uno de la clase $C_b$, se suman, la suma siempre es un entero en una clase única, a saber $C_{a+b}$ o bien $C_{a+b-m}$ de acuerdo con que $a+b<m$ o bien $a+b \geqq m$. En consecuencia, definir la suma $C_a + C_b = C_{a+b}$ o bien $C_a + C_b = C_{a+b-m}$ y probar que estas clases forman un grupo bajo esta adición. Probar que este grupo es isomorfo al grupo aditivo módulo $m$.

## 2.11 Grupos multiplicativos, anillos y campos

**Teorema 2.30** *Sea $m > 1$ un entero positivo. Cualquier sistema reducido de residuos módulo $m$ es un grupo bajo la multiplicación módulo $m$. El grupo es de orden $\phi(m)$. Dos grupos cualesquiera de ese tipo son isomorfos y así, se habla de "el grupo multiplicativo módulo $m$".*

*Demostración.* Consideremos cualquier sistema reducido de residuos $r_1, r_2, \ldots, r_n$ donde $n = \phi(m)$. Este conjunto es cerrado bajo la multiplicación módulo $m$ por el Teorema 1.8. La propiedad asociativa de la multiplicación se hereda de la propiedad correspondiente para los en-

teros, porque $a(bc) = (ab)c$ implica que $a(bc) \equiv (ab)c \pmod{m}$. El sistema reducido de residuos contiene un elemento, digamos $r_j$, tal que $r_j \equiv 1 \pmod{m}$ y éste es, evidentemente, el elemento identidad único del grupo. Finalmente, para cada $r_j$, la congruencia $xr_i \equiv r_j \pmod{m}$ tiene una solución, por el Teorema 2.13, y esta solución es única dentro del sistema reducido de residuos $r_1, r_2, \ldots, r_n$. Dos sistemas reducidos diferentes de residuos módulo $m$ son congruentes, elemento por elemento, módulo $m$, y así se tiene un isomorfismo entre los dos grupos.

*Notación.* Hemos estado usando el símbolo $\oplus$ para la operación binaria del grupo y hemos encontrado que, en grupos particulares, $\oplus$ puede representar la adición, la multiplicación o alguna otra operación. Al manejar grupos generales es conveniente eliminar el símbolo $\oplus$, así como en el álgebra generalmente se omite el punto que representa la multiplicación ordinaria. Se escribirá $ab$ por $a \oplus b$, $abc$ por $a \oplus (b \oplus c) = (a \oplus b) \oplus c$, $a^2$ por $a \oplus a$, $a^3$ por $a \oplus (a \oplus a)$, etc. También puede escribirse $abcd$ por $(a \oplus b \oplus c) \oplus d = (a \oplus b) \oplus (c \oplus d)$ etc., tal y como puede verse aplicando la inducción a la ley asociativa. Es más, se usará la palabra multiplicación para la operación $\oplus$, pero debe recordarse que no se refiere a la multiplicación ordinaria de la aritmética. De hecho, estaremos trabajando con grupos generales, de modo que $a$ no es un número, solamente es un elemento abstracto de un grupo. Es conveniente escribir $a^0$ por $e$, $a^{-2}$ por $(a^{-1})^2$, $a^{-3}$ por $(a^{-1})^3$, etc. No es difícil demostrar que las leyes de los exponentes usuales son válidas bajo esta definición.

**Teorema 2.31** *En cualquier grupo, $G$, $ab = ac$ implica $b = c$. Si $a$ es cualquier elemento de un grupo finito $G$ con elemento identidad $e$, entonces existe un menor entero positivo $r$ (único) tal que $a^r = e$.*

*Demostración.* La primera parte del teorema se establece al multiplicar por la izquierda $ab = ac$ por $a^{-1}$, así $a^{-1}(ab) = a^{-1}(ac)$, $(a^{-1}a)b = (a^{-1}a)c$, $eb = ec$, $b = c$. Para probar la segunda parte, considérese la serie de elementos obtenida mediante la multiplicación repetida por $a$,

$$e, a, a^2, a^3, a^4, \ldots .$$

Dado que el grupo es finito y ya que los miembros de esta serie son elementos del grupo, debe ocurrir una repetición de la forma $a^s = a^t$ con, digamos, $s < t$. Pero esta ecuación puede escribirse en la forma $a^s e = a^s a^{t-s}$, de donde $a^{t-s} = e$. Así que existe algún entero positivo, $t - s$, tal que $a^{t-s} = e$ y el menor exponente positivo con esta propiedad es el valor de $r$ en el teorema.

**Definición 2.11** *Sea $G$ cualquier grupo, finito o infinito, y $a$ un elemento de $G$. Si $a^s = e$ para algún entero positivo $s$, entonces se dice*

*que a es de orden finito.* ***Si a es de orden finito,*** *el orden de a es el menor entero positivo r tal que* $a^r = e$. *Si no existe entero positivo s tal que* $a^s = e$, *entonces se dice que a es de orden infinito. Se dice que un grupo G es cíclico si contiene un elemento a tal que las potencias de a*

$$\ldots, a^{-3}, a^{-2}, a^{-1}, a^0 = e, a, a^2, a^3, \ldots$$

*comprenden al grupo completo; se dice que tal elemento genera al grupo y recibe el nombre de generador.*

El Teorema 2.31 demuestra que todos los elementos de un grupo finito son de orden finito. Todo grupo, finito o infinito, contiene por lo menos al elemento $e$ que es de orden finito. Existen grupos infinitos que consisten completamente de elementos de orden finito.

Si un grupo cíclico es finito y tiene generador $a$, entonces el grupo consiste de $e, a, a^2, a^3, \ldots, a^{r-1}$, donde $r$ es el orden del elemento $a$. Todas las demás potencias de $a$ son superfluas porque simplemente son repeticiones de éstas.

**Teorema 2.32** *El orden de un elemento de un grupo finito G es un divisor del orden del grupo. Si el orden del grupo se denota por n, entonces* $a^n = e$.

*Demostración.* Supóngase que el elemento $a$ tiene el orden $r$. Fácilmente se ve que

$$(A) \qquad e, a, a^2, a^3, \ldots, a^{r-1}$$

son $r$ elementos distintos de $G$. Si estos $r$ elementos no agotan el grupo, existe algún otro elemento, digamos $b_2$. Entonces puede probarse que

$$(B) \qquad b_2, b_2a, b_2a^2, b_2a^3, \ldots, b_2a^{r-1}$$

son $r$ elementos distintos, todos diferentes de los $r$ elementos de $A$. Porque, en primer lugar, si $b_2a^s = b_2a^t$, entonces, por el Teorema 2.31, $a^s = a^t$. Y, por otra parte, si $b_2a^s = a^t$, entonces $b_2 = a^{t-s}$, de modo que $b_2$ estaría entre las potencias de $a$.

Si $G$ no es agotado por los conjuntos $A$ y $B$, entonces existe otro elemento $b_3$ que llevará a $r$ nuevos elementos

$$b_3, b_3a, b_3a^2, b_3a^3, \ldots, b_3a^{r-1},$$

todos diferentes de los elementos de $A$ y $B$, mediante un argumento semejante. Este proceso de obtener nuevos elementos $b_2, b_3, \ldots$ debe terminar supuesto que $G$ es finito. De modo que si la última hornada de elementos nuevos es, digamos

$$b_k, b_ka, b_ka^2, b_ka^3, \ldots, b_ka^{r-1},$$

entonces el orden del grupo $G$ es $kr$ y queda demostrada la primera parte del teorema. Para probar la segunda parte, se observa que $n = kr$ y $a^r = e$, por el Teorema 2.31, de donde $a^n = e$.

Puede observarse que el Teorema 2.32 implica los teoremas de Fermat y de Euler, donde se toma como el grupo al conjunto de enteros relativamente primos al módulo $m$. Al introducir esta implicación, el lector verá la necesidad de "traducir" el lenguaje y la notación de la teoría de grupos a la de la teoría de los números. En la misma forma se observa que el lenguaje de la Definición 2.7, que "$a$ pertenece al exponente $h$ módulo $m$", se traduce al lenguaje teórico de los grupos como "el elemento $a$ del grupo multiplicativo módulo $m$ tiene orden $h$". También, la "raíz primitiva módulo $m$" de la Definición 2.8 se llama "generador" del grupo multiplicativo módulo $m$ en la teoría de los grupos.

**Definición 2.12** *Un anillo es un conjunto de por lo menos dos elementos con dos operaciones binarias,* $\oplus$ *y* $\odot$, *tal que es un grupo conmutativo bajo* $\oplus$, *es cerrado bajo* $\odot$, *y tal que* $\odot$ *es asociativa y distributiva respecto a* $\oplus$. *El elemento identidad respecto a* $\oplus$ *recibe el nombre de "cero" del anillo. Si todos los elementos de un anillo, que no sean el cero, forman un grupo conmutativo bajo* $\odot$, *entonces recibe el nombre de campo.*

Se acostumbra llamar adición a $\oplus$ y multiplicación a $\odot$ y escribir $a + b$ por $a \oplus b$, $ab$ por $a \odot b$. Entonces, las condiciones sobre $\odot$ para un anillo son $a(bc) = (ab)c$, $a(b + c) = ab + ac$, $(b + c)a = ba + ca$. En general, los elementos $a, b, c, \cdots$ no son números y las operaciones de la adición y la multiplicación no son las ordinarias de la aritmética. Sin embargo, los únicos anillos y campos que se considerarán aquí tendrán números como elementos y las operaciones serán la adición y la multiplicación ordinarias o bien la adición y la multiplicación módulo $m$.

**Teorema 2.33** *El conjunto* $I_m$ *de elementos* $0, 1, 2, \cdots, m - 1$, *con la adición y la multiplicación módulo m definidas, es un anillo para cualquier entero* $m > 1$. *Tal anillo es un campo si y solamente si m es primo.*

*Demostración.* Ya se ha demostrado en el Teorema 2.29 que cualquier sistema completo de residuos módulo $m$ es un grupo bajo la adición módulo $m$. Este grupo es conmutativo y las propiedades asociativa y distributiva de la multiplicación módulo $m$ se heredan de las propiedades correspondientes para la multiplicación ordinaria. Por lo tanto $I_m$ es un anillo.

A continuación, por el Teorema 2.30, cualquier sistema reducido de residuos módulo $m$ es un grupo bajo la multiplicación módulo $m$. Si $m$

es un primo $p$, el sistema reducido de residuos de $I_p$ es $1, 2, \cdots, p-1$, esto es, todos los elementos de $I_p$ diferentes a 0. Dado que 0 es el cero del anillo, $I_p$ es un campo. Por otra parte, si $m$ no es primo, entonces $m$ es de la forma $ab$ con $1 < a \leqq b < m$. Entonces los elementos de $I_m$ diferentes de 0 no forman un grupo bajo la multiplicación módulo $m$ debido a que no existe inverso para el elemento $a$, ni solución de $ax \equiv 1 \pmod{m}$. De donde $I_m$ no es un campo.

**Problemas**

1. Probar que el grupo multiplicativo módulo 9 es isomorfo al grupo aditivo módulo 6.
2. Probar que el grupo aditivo módulo $m$ es cíclico con 1 como generador. Probar que todos los primos relativos a $m$, menores que $m$ pueden servir como generador.
3. Probar que dos grupos cíclicos cualesquiera de orden $m$ son isomorfos.
4. Probar que el grupo de todos los enteros bajo la adición es un grupo cíclico infinito.
5. Si $a$ es un elemento de orden $r$ de un grupo $G$, probar que $a^k = e$ si y solamente si $r|k$.
6. ¿Cuál es el menor entero positivo $m$ tal que el grupo multiplicativo módulo $m$ no es cíclico?
7. Un subgrupo $S$ de un grupo $G$ es un subconjunto de elementos de $G$ los cuales forman un grupo bajo la misma operación binaria. Si $G$ es finito, probar que el orden de un subgrupo $S$ es un divisor del orden de $G$.
8. Probar el Teorema 2.32 en forma análoga a la demostración del Teorema 2.8.
9. Probar el Teorema 2.8 por el método usado en la demostración del Teorema 2.32.
10. Supóngase que $G$ consiste de todas las sucesiones posibles $(a_1, a_2, a_3, \cdots)$ con cada $a_i = 1$ o bien $-1$. Sea $(a_1, a_2, a_3, \cdots) \oplus (b_1, b_2, b_3, \cdots) = (a_1b_1, a_2b_2, a_3b_3, \cdots)$. Demostrar que $G$ es un grupo infinito en el cual todos los elementos son de orden finito.
11. Supóngase que $G$ consiste de $a, b, c, d, e, f$ y sea $\oplus$ definida mediante la siguiente tabla.

| $\oplus$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $d$ | $f$ |
| $a$ | $a$ | $e$ | $d$ | $f$ | $b$ | $c$ |
| $b$ | $b$ | $f$ | $e$ | $d$ | $c$ | $a$ |
| $c$ | $c$ | $d$ | $f$ | $e$ | $a$ | $b$ |
| $d$ | $d$ | $c$ | $a$ | $b$ | $f$ | $e$ |
| $f$ | $f$ | $b$ | $c$ | $a$ | $e$ | $d$ |

Demostrar que $G$ es un grupo no conmutativo.

12. Probar que el grupo multiplicativo módulo $p$ es cíclico si $p$ es primo.
13. Construir las tablas de adición y multiplicación para los elementos del campo de residuos módulo 7.

14. Probar que el conjunto de todos los enteros bajo la adición y la multiplicación ordinarias es un anillo pero no un campo.
15. Probar que el conjunto de todos los enteros pares bajo la adición y la multiplicación ordinarias es un anillo.
16. Probar que el conjunto 0, 3, 6, 9 es un anillo bajo la adición y la multiplicación módulo 12.
17. Probar que en cualquier campo $a0 = 0a = 0$ para todo elemento $a$.
18. Sea $a$ un divisor de $m$, digamos $m = aq$ con $1 < a < m$. Probar que el conjunto de elementos, $0, a, 2a, 3a, \cdots, (q-1)a$, con la adición y la multiplicación módulo $m$, forma un anillo. ¿Bajo qué circunstancias es un campo?
19. Probar que el conjunto de todos los números racionales forma un campo.
20. Probar que el conjunto de todas las funciones racionales $f(x)/g(x)$, donde $f(x)$ y $g(x)$ son polinomios con coeficientes enteros y $g(x) \not\equiv 0$, forma un campo.
21. Si $x, y, z$ son números cualesquiera, reales o complejos, la ley de cancelación establece que $xy = xz$ implica $y = z$ si $x \neq 0$. Existe una ley de cancelación "débil" que establece que $x^2y = x^2z$ implica que $xy = xz$ sea $x$ igual a cero o no. Considérese el conjunto de todos los enteros módulo $m$ con la multiplicación módulo $m$, $m > 1$. Demostrar que la ley de cancelación se cumple si y solamente si $m$ es primo y que la ley "débil" se cumple si y solamente si $m$ es exento de cuadrados, esto es, $m$ es un producto de primos distintos.
22. Considérese el sistema de todos los enteros módulo $m$ bajo la multiplicación módulo $m$, $m > 1$. Demostrar que:
    *a*) No es un grupo.
    *b*) Es asociativo.
    *c*) Es conmutativo.
    *d*) Es cerrado.
    *e*) Tiene una unidad única—un elemento $u$ tal que $ux = x$ para todo $x$.
    *f*) Tiene un cero único—un elemento $z$ tal que $zx = z$ para todo $x$.
23. Para $m = 30$ encontrar todos los elementos idempotentes ($x$ tales que $x^2 = x$). También encontrar los elementos $w$ tales que $wx = z$, el elemento cero, para algún $x \neq z$.
24. Un dominio entero es un anillo con las siguientes propiedades adicionales: (i) existe un elemento identidad único respecto a la multiplicación; (ii) la multiplicación es conmutativa; (iii) si $ab = ac$ y $a \neq 0$, entonces $b = c$. Probar que cualquier campo es un dominio entero. ¿Cuáles de los siguientes conjuntos son dominios enteros?:
    (*a*) el conjunto de todos los enteros;
    (*b*) el conjunto $I_m$ del Teorema 2.33;
    (*c*) el conjunto $F[x]$ de todos los polinomios en una variable o indeterminada $x$, con coeficientes en un campo $F$.
25. Sea $m$ un entero positivo y considérese el conjunto de todos los divisores de $m$. Definir dos operaciones para los números de este conjunto, $\odot$ y $\oplus$, como $a \odot b = (a, b)$, $a \oplus b = [a, b]$, m.c.d. y m.c.m. respectivamente. Probar que $\odot$ y $\oplus$ son asociativas y conmutativas. Probar la ley distributiva $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$ y su dual $a \oplus (b \odot c) = (a \oplus b) \odot (a \oplus c)$. Demostrar que $a \odot a = a \oplus a = a$. También probar que $1 \odot a = 1$ y $1 \oplus a = a$, de manera que 1 se comporta como un

cero ordinario, y $m \odot a = a$ y $m \oplus a = m$. Definir una relación ⧀ como $a$ ⧀ $b$ si $a \odot b = a$. Probar que $a$ ⧀ $a$, que ⧀ es transitiva y que $a$ ⧀ $b$ si y solamente si $a \oplus b = b$.

Probar que si $m$ no es divisible entre cualquier cuadrado excepto 1, entonces correspondiendo a cada divisor $a$ existe un divisor $a'$ tal que $a \odot a' = 1$, $a \oplus a' = m$. (Estas álgebras con $m$ exento de cuadrados son ejemplos de álgebras booleanas).

# Capítulo 3

# Reciprocidad cuadrática

## 3.1 Residuos cuadráticos

**Definición 3.1** *Para todo $a$ tal que $(a, m) = 1$, $a$ recibe el nombre de residuo cuadrático módulo $m$ si la congruencia $x^2 \equiv a \pmod{m}$ tiene una solución. Si no tiene solución, entonces $a$ se llama no residuo cuadrático módulo $m$.*

Dado que $a + m$ es un residuo o bien un no residuo cuadrático módulo $m$ de acuerdo con que $a$ sea o no lo sea, solamente consideraremos residuos o bien no residuos distintos aquellos que sean de distinto módulo $m$. Los residuos cuadráticos módulo 5 son 1 y 4 mientras que 2 y 3 son los no residuos.

**Definición 3.2** *Si $p$ denota un primo impar y $(a, p) = 1$, el símbolo de Legendre $\left(\frac{a}{p}\right)$ se define como 1 si $a$ es un residuo cuadrático, $-1$ si $a$ es un no residuo cuadrático módulo $p$.*

**Teorema 3.1** *Sea $p$ un primo impar y supóngase que $a$ y $b$ denotan enteros relativamente primos para $p$. Entonces*

(*a*) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$,

(*b*) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,

(*c*) $a \equiv b$ (mód $p$) *implica que* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(*d*) $\left(\frac{a^2}{p}\right) = 1, \quad \left(\frac{1}{p}\right) = 1, \quad \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

*Demostración.* La parte ($a$) del teorema se deduce del Corolario 2.28. Las partes restantes son todas simples consecuencias de la parte ($a$). La parte ($a$) también puede probarse sin usar el Corolario 2.28. Si $\left(\frac{a}{p}\right) = 1$, entonces $x^2 \equiv a \pmod p$ tiene una solución, digamos $x_0$. Por el Teorema 2.7, $a^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod p$.

Por otra parte, si $\left(\frac{a}{p}\right) \equiv -1$, entonces $x^2 \equiv a \pmod p$ no tiene solución y se procede como en la demostración del Teorema 2.10. A cada $j$ que satisfaga $1 \leqq j \leqq p - 1$ se asocia el entero único $i$ tal que $ji \equiv a \pmod p$, $0 \leqq i \leqq p - 1$. Se ve que $i = 0$ es imposible y que el asociado de $i$ es $j$. Dado que $x^2 \equiv a \pmod p$ no tiene solución, ningún entero $j$ se asocia consigo mismo. Por lo tanto, los enteros $1, 2, \ldots, p - 1$ pueden parearse, $j$ y su asociado $i$, y $ji \equiv a \pmod p$. Se tiene $(p - 1)/2$ pares. Multiplicando juntos a todos estos pares se obtiene $(p - 1)! \equiv a^{(p-1)/2} \pmod p$. Usando el Teorema 2.10 se obtiene $a^{(p-1)/2} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p$.

**Teorema 3.2** *Lema de Gauss. Sea $p$ un primo impar y sea $(a, p) = 1$. Considérense los enteros $a, 2a, 3a, \ldots, \{(p - 1)/2\} a$ y sus menores residuos no negativos módulo $p$. Si $n$ denota el número de estos residuos que exceden a $\frac{p}{2}$, entonces $\left(\frac{a}{p}\right) = (-1)^n$.*

*Demostración.* Denotemos por $r_1, r_2, \ldots, r_n$ los residuos que exceden a $p/2$ y denotemos por $s_1, s_2, \ldots, s_k$ los residuos restantes. Los $r_i$ y los $s_i$ son todos distintos y ninguno es cero. Además $n + k = (p - 1)/2$. Ahora bien, $0 < p - r_i < p/2$, $i = 1, 2, \ldots, n$ y los números $p - r_i$ son distintos. También ningún $p - r_i$ es un $s_j$ porque si $p - r_i = s_j$ entonces $r_i \equiv \rho a$, $s_j \equiv \sigma a$, para algunos $\rho, \sigma$, $1 \leqq \rho \leqq (p - 1)/2$, $1 \leqq \sigma \leqq (p - 1)/2$ y $p - \rho a \equiv \sigma a \pmod p$. Supuesto que $(a, p) = 1$ esto implica que $a(\rho + \sigma) \equiv 0$, $\rho + \sigma \equiv 0 \pmod p$, lo cual es imposible. Por tanto, $p - r_1, p - r_2 \cdots; p - r_n, s_1 s_2, \ldots, s_k$ son todos distintos, son todos por lo menos iguales a 1 y menores que $p/2$ y en número son $n + k = (p - 1)/2$. Esto es, existen solamente los enteros $1, 2, \ldots, (p - 1)/2$ en algún orden. Multiplicándolos juntos se tiene

$$(p - r_1)(p - r_2) \cdots (p - r_n) s_1 s_2 \cdots s_k = 1 \cdot 2 \cdots \frac{p-1}{2}$$

y entonces

$$(-r_1)(-r_2) \cdots (-r_n) s_1 s_2 \cdots s_k \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \pmod{p},$$

$$(-1)^n r_1 r_2 \cdots r_n s_1 s_2 \cdots s_k \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \pmod{p},$$

$$(-1)^n a \cdot 2a \cdot 3a \cdots \frac{p-1}{2} a \equiv 1 \cdot 2 \cdots \frac{p-1}{2} \pmod{p}.$$

Pueden cancelarse los factores 2, 3, . . . , $(p-1)/2$ para obtener $(-1)^n a^{(p-1)/2} \equiv 1 \pmod{p}$ lo cual, por el Teorema 3.1*a*, nos da $(-1)^n \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

**Definición 3.3** *Para x real, el símbolo* $[x]$ *denota el máximo entero menor que o igual a x.*

Por ejemplo, $[15/2] = 7$, $[-15/2] = -8$, $[-15] = -15$.

**Teorema 3.3** *Si p es un primo impar y* $(a, 2p) = 1$, *entonces*

$$\left(\frac{a}{p}\right) = (-1)^t \quad \textit{donde} \quad t = \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right], \quad y \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

*Demostración.* Usaremos la misma notación usada en la demostración del Teorema 3.2. Los $r_i$ y los $s_i$ son precisamente los menores residuos positivos al dividir los enteros $ja$ entre $p$, $j = 1, 2, \ldots, (p-1)/2$. Fácilmente se ve que el cociente en esta división es $q = [ja/p]$. Entonces, para $(a, p) = 1$, sea $a$ impar o bien par, se tiene

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p\left[\frac{ja}{p}\right] + \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j$$

y

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{n} (p - r_j) + \sum_{j=1}^{k} s_j = np - \sum_{j=1}^{n} r_j + \sum_{j=1}^{k} s_j$$

y de aquí que restando,

$$(a-1)\sum_{j=1}^{(p-1)/2} j = p\left(\sum_{j=1}^{(p-1)/2}\left[\frac{ja}{p}\right] - n\right) + 2\sum_{j=1}^{n} r_j.$$

Pero

$$\sum_{j=1}^{(p-1)/2} j = \frac{p^2-1}{8}$$

así que se tiene

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right] - n \pmod 2.$$

si $a$ es impar, esto implica $n \equiv \sum_{j=1}^{(p-1)/2} \left[\frac{ja}{p}\right] \pmod 2$. Si $a = 2$ implica $n \equiv (p^2-1)/8 \pmod 2$ ya que $[2j/p] = 0$ para $1 \leqq j \leqq (p-1)/2$. Ahora el teorema se deduce del Teorema 3.2.

**Problemas**

1. Encontrar $[3/2]$, $[-3/2]$, $[\pi]$, $[-7]$, $[x]$ para $0 \leqq x < 1$.
2. Con referencia a la notación del Teorema 1.2 probar que $q = [b/a]$.
3. Probar que 3 es un residuo cuadrático de 13 pero un no residuo cuadrático de 7.
4. Encontrar los valores de $\left(\frac{a}{p}\right)$ en cada uno de los 12 casos, $a = -1, 2, -2, 3$ y $p = 11, 13, 17$.
5. Probar que los residuos cuadráticos de 11 son 1, 3, 4, 5, 9 y enlistar todas las soluciones de cada una de las diez congruencias $x^2 \equiv a \pmod{11}$ y $x^2 \equiv a \pmod{11^2}$ donde $a = 1, 3, 4, 5, 9$.
6. Enlistar los residuos cuadráticos de cada uno de los primos 7. 13, 17, 29 37.
7. ¿Cuáles de las siguientes congruencias tienen soluciones? ¿Cuántas?

   *a*) $x^2 \equiv 2 \pmod{61}$ *b*) $x^2 \equiv 2 \pmod{59}$
   *c*) $x^2 \equiv -2 \pmod{61}$ *d*) $x^2 \equiv -2 \pmod{59}$
   *e*) $x^2 \equiv 2 \pmod{122}$ *f*) $x^2 \equiv 2 \pmod{118}$
   *g*) $x^2 \equiv -2 \pmod{122}$ *h*) $x^2 \equiv -2 \pmod{118}$.

8. ¿Cuántas soluciones se tienen para cada una de las siguientes congruencias?

   *a*) $x^2 \equiv -1 \pmod{61}$ *b*) $x^2 \equiv -1 \pmod{59}$
   *c*) $x^2 \equiv -1 \pmod{365}$ *d*) $x^2 \equiv -1 \pmod{3599}$
   *e*) $x^2 \equiv -1 \pmod{122}$ *f*) $x^2 \equiv -1 \pmod{244}$.

9. Sean $p$ un primo y $(a, p) = (b, p) = 1$. Probar que si $x^2 \equiv a \pmod p$ y $x^2 \equiv b \pmod p$ no son resolubles, entonces $x^2 \equiv ab \pmod p$ sí puede resolverse.
10. Probar que si $p$ es un primo impar entonces $x^2 \equiv 2 \pmod p$ tiene soluciones si y solamente si $p \equiv 1$ o bien $7 \pmod 8$.
11. Denotar los residuos cuadráticos por $r$, los no residuos por $n$. Probar que $r_1r_2$ y $n_1n_2$ son residuos y que $rn$ es un no residuo para un primo $p$. Demostrar que existen $(p-1)/2$ residuos cuadráticos y $(p-1)/2$ no residuos para un primo impar $p$.

12. Sea $g$ una raíz primitiva de un primo impar $p$. Probar que los residuos cuadráticos módulo $p$ son congruentes a $g^2, g^4, g^6, \cdots, g^{p-1}$ y los no residuos son congruentes a $g, g^3, g^5, g^7, \cdots, g^{p-2}$.
13. Probar que si $r$ es un residuo cuadrático módulo $m$, entonces $r^{\phi(m)/2} \equiv 1 \pmod{m}$. *Sugerencia*: usar el hecho de que existe algún entero $a$ tal que $r \equiv a^2 \pmod{m}$.
14. Demostrar que si $a$ es un residuo cuadrático módulo $m$ y $ab \equiv 1 \pmod{m}$, entonces $b$ también es un residuo cuadrático. A continuación probar que el producto de los residuos cuadráticos módulo $p$ es congruente a $+1$ o bien a $-1$ de acuerdo con que el primo $p$ sea de la forma $4k + 3$ o bien $4k + 1$.
15. Probar que si $p$ es un primo que tiene la forma $4k + 3$ y si $m$ es el número de residuos cuadráticos menores que $p/2$, entonces $1 \cdot 3 \cdot 5 \cdots (p-2) \equiv (-1)^{m+k+1} \pmod{p}$ y $2 \cdot 4 \cdot 6 \cdots (p-1) \equiv (-1)^{m+k} \pmod{p}$.
16. Probar que los residuos cuadráticos módulo $p$ son congruentes a $1^2, 2^2, 3^2, \cdots, \{(p-1)/2\}^2$. De aquí probar que si $p > 3$, la suma de los residuos cuadráticos es divisible entre $p$.
17. Para todos los primos $p$ probar que $x^8 \equiv 16 \pmod{p}$ es posible. *Sugerencia*: aplicar el Teorema 2.27.
18. Sea $p$ un primo impar. Probar que si existe un entero $x$ tal que

$p|(x^2 + 1)$ entonces $p \equiv 1 \pmod{4}$;
$p|(x^2 - 2)$ entonces $p \equiv 1$ ó $7 \pmod{8}$;
$p|(x^2 + 2)$ entonces $p \equiv 1$ ó $3 \pmod{8}$;
$p|(x^4 + 1)$ entonces $p \equiv 1 \pmod{8}$.

Demostrar que existe un número infinito de primos de cada una de las formas $8n + 1$, $8n + 3$, $8n + 5$, $8n + 7$. *Sugerencia*: aplicar el Teorema 2.27 para el caso $p|(x^4 + 1)$.

## 3.2 Reciprocidad cuadrática

**Teorema 3.4** *Ley gaussiana de la reciprocidad. Si p y q son primos impares distintos, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)}{2}\frac{(q-1)}{2}}$$

*Demostración.* Sea $S$ el conjunto de todos los pares de enteros $(x, y)$ los cuales satisfacen $1 \leqq x \leqq (p-1)/2$, $1 \leqq y \leqq (q-1)/2$. El conjunto $S$ tiene $(p-1)(q-1)/4$ miembros. Sepárese este conjunto en dos subconjuntos mutuamente excluyentes $S_1$ y $S_2$ de acuerdo a que $qx > py$ o bien $qx < py$. Nótese que no existen pares $(x, y)$ en $S$ tales que $qx = py$. El conjunto $S_1$ puede describirse como el conjunto de todos los pares $(x, y)$ tales que $1 \leqq x \leqq (p-1)/2$, $1 \leqq y < qx/p$. Entonces se ve que el número de pares en $S_1$ es $\sum_{x=1}^{(p-1)/2} [qx/p]$. Del mismo modo $S_2$ consiste de todos los pares $(x, y)$ tales que $1 \leqq y \leqq (q-1)/2$, $1 \leqq x < py/q$ y el número de pares en $S_2$ es $\sum_{y=1}^{(q-1)/2} [py/q]$. Así se tiene

$$\sum_{j=1}^{(p-1)/2}\left[\frac{qj}{p}\right]+\sum_{j=1}^{(q-1)/2}\left[\frac{pj}{q}\right]=\frac{p-1}{2}\frac{q-1}{2}$$

y de aquí que

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\{(p-1)/2\}\{(q-1)/2\}}$$

por el Teorema 3.3,

Este teorema junto con el Teorema 3.1 y la segunda parte del Teorema 3.3 hace que el cálculo de $\left(\frac{a}{p}\right)$ sea medianamente sencillo. Por ejemplo, se tiene

$$\left(\frac{-42}{61}\right)=\left(\frac{-1}{61}\right)\left(\frac{2}{61}\right)\left(\frac{3}{61}\right)\left(\frac{7}{61}\right),$$

$$\left(\frac{-1}{61}\right)=(-1)^{60/2}=1,$$

$$\left(\frac{2}{61}\right)=(-1)^{(61^2-1)/8}=-1,$$

$$\left(\frac{3}{61}\right)=\left(\frac{61}{3}\right)(-1)^{(2/2)(60/2)}=\left(\frac{1}{3}\right)=1,$$

$$\left(\frac{7}{61}\right)=\left(\frac{61}{7}\right)(-1)^{(6/2)(60/2)}=\left(\frac{5}{7}\right)=\left(\frac{7}{5}\right)(-1)^{(4/2)(6/2)}=\left(\frac{2}{5}\right)$$

$$=(-1)^{24/8}=-1$$

De aquí que $\left(\frac{-42}{61}\right)=1$. Este cálculo muestra un número de diferentes tipos de pasos; se escogió con ese objeto y no es el más corto posible Un camino más corto es

$$\left(\frac{-42}{61}\right)=\left(\frac{19}{61}\right)=\left(\frac{61}{19}\right)\cdot 1=\left(\frac{4}{19}\right)=1.$$

También podría obtenerse el valor de $\left(\frac{-42}{61}\right)$ mediante la aplicación del Teorema 3.2 o la primera parte del Teorema 3.3 pero el cálculo sería considerablemente más largo.

Existe otro tipo de problema de cierta importancia. Por ejemplo, encontremos todos los primos impares $p$ tales que 3 es un residuo cuadrático módulo $p$. Se tiene

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{(p-1)/2},$$

$$\left(\frac{p}{3}\right) = \begin{cases} \left(\frac{1}{3}\right) = 1 \text{ si } p \equiv 1 \pmod{3} \\ \left(\frac{2}{3}\right) = -1 \text{ si } p \equiv 2 \pmod{3}, \end{cases}$$

y

$$(-1)^{(p-1)/2} = \begin{cases} 1 \text{ si } p \equiv 1 \pmod{4} \\ -1 \text{ si } p \equiv 3 \pmod{4}. \end{cases}$$

Por tanto $\left(\frac{3}{p}\right) = 1$ si y solamente si $p \equiv 1 \pmod 3$, $p \equiv 1 \pmod 4$ o bien $p \equiv 2 \pmod 3$, $p \equiv 3 \pmod 4$; es decir $p \equiv 1$ o bien $11 \pmod{12}$.

En ocasiones, resultados de este tipo son útiles cuando se trata de determinar si un cierto número es primo o no. Considérese el número 9997. Podría observarse que $9997 = 100^2 - 3$, de modo que $3 \equiv 100^2 \pmod p$ si $p|9997$. Esto es si $p =$ o bien $\left(\frac{3}{p}\right) = 1$. Dado que $3 \not| 9997$ se tiene $\left(\frac{3}{p}\right) = 1$ y de aquí que $p \equiv 1$ o bien $11 \pmod{12}$. Solamente es necesario ensayar los $p$ tales que $p \leqq \sqrt{9997}$. Si se enlistan los números 1, 13, 25, . . . , 97 y 11, 23, 35, . . . , 95 puede eliminarse 1 y todos los números compuestos y se encuentran precisamente los once primos que deben ensayarse. Se encontrará que 13 divide a 9997 y que $9997 = 13 \cdot 769$ ¿Es primo 769? Si $p|769$ entonces $p|9997$ y se encontrará en nuestra lista. Los únicos $p$ en nuestra lista tales que $p \leqq \sqrt{769}$ son 13, 11 y 23. Ninguno de éstos divide a 769 y de aquí que 769 es primo.

**Problemas**

1. En el ejemplo precedente ¿por qué es innecesario probar los primos $p > \sqrt{9997}$?
2. Probar que si $p$ y $q$ son primos de la forma $4k + 3$ y si $x^2 \equiv p \pmod q$ no tiene soluciones, entonces $x^2 \equiv q \pmod p$ tiene dos soluciones.
3. Probar que si un primo $p$ es un residuo cuadrático de un primo impar $q$ y $p$ es de la forma $4k + 1$ entonces $q$ es un residuo cuadrático de $p$.
4. ¿Cuáles de las siguientes congruencias pueden resolverse?

   *a*) $x^2 \equiv 5 \pmod{227}$ *b*) $x^2 \equiv 5 \pmod{229}$
   *c*) $x^2 \equiv -5 \pmod{227}$ *d*) $x^2 \equiv -5 \pmod{229}$
   *e*) $x^2 \equiv 7 \pmod{1009}$ *f*) $x^2 \equiv -7 \pmod{1009}$

   (Nótese que 227, 229 y 1009 son primos.)

5. Encontrar los valores de $\left(\frac{p}{q}\right)$ en los nueve casos obtenidos de todas las combinaciones de $p = 7$, 11, 13 y $q = 227$, 229 y 1009.
6. Determinar si $x^2 \equiv 150 \pmod{1009}$ puede o no resolverse.
7. Encontrar todos los primos $p$ tales que $x^2 \equiv 11 \pmod{p}$ tiene una solución.
8. Encontrar todos los primos $p$ tales que $\left(\frac{10}{p}\right) = 1$.
9. Encontrar todos los primos $p$ tales que $\left(\frac{5}{p}\right) = -1$.
10. ¿De cuáles primos $-2$ es un residuo cuadrático?
11. Si $a$ es un no residuo cuadrático de cada uno de los primos impares $p$ y $q$ ¿puede resolverse $x^2 \equiv a \pmod{pq}$?
12. En la demostración del Teorema 3.4 considérense los pares $(x, y)$ como puntos en un plano. Denótese por $O$, $A$, $B$, $C$ los puntos $(0, 0)$, $(p/2, 0)$, $(p/2, q/2)$, $(0, q/2)$, respectivamente y trácense las rectas $OA$, $OB$, $OC$, $AB$ y $BC$. Repítase la demostración del Teorema 3.4 usando lenguaje geométrico — pares de puntos, etc.
13. Probar que existe un número infinito de primos de cada una de las formas $3n + 1$ y $3n - 1$. *Sugerencia*: primero determínense los primos $p$ tales que $\left(\frac{-3}{p}\right) = 1$.

## 3.3 El símbolo de Jacobi

**Definición 3.4** *Sea* $(P, Q) = 1$, $Q > 0$, $Q$ *impar, de modo que* $Q = q_1 q_2 \cdots q_s$ *donde los* $q_i$ *son primos impares, no necesariamente distintos. Entonces el símbolo de Jacobi* $\left(\frac{P}{Q}\right)$ *está definido por*

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s} \left(\frac{P}{q_j}\right)$$

*donde* $\left(\frac{P}{q_j}\right)$ *es el símbolo de Legendre.*

Si $Q$ es un primo impar, el símbolo de Jacobi y el símbolo de Legendre son indistinguibles. Sin embargo, esto no puede causar confusión dado que sus valores son los mismos en este caso. Evidentemente $\left(\frac{P}{Q}\right) = \pm 1$ pero no es cierto que $\left(\frac{P}{Q}\right) = 1$ implica que $P$ sea un residuo cuadrático módulo $Q$. Por ejemplo, $\left(\frac{2}{9}\right) = 1$ pero $x^2 \equiv 2 \pmod 9$ no tiene solución. Un número $a$ es un residuo cuadrático módulo $Q$ solamente si $(a, Q) = 1$ y $a$ es un residuo cuadrático módulo todos los primos $p$ que dividen a $Q$. *Si* $\left(\frac{a}{Q}\right) = -1$, entonces $a$ no es un residuo cuadrático.

**Teorema 3.5** *Supóngase que $Q$ y $Q'$ son impares y positivos y que* $(PP', QQ') = 1$. *Entonces*

(*a*) $\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$,

(*b*) $\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$,

(*c*) $\left(\frac{P^2}{Q}\right) = \left(\frac{P}{Q^2}\right) = 1$,

(*d*) $\left(\frac{P'P^2}{Q'Q^2}\right) = \left(\frac{P'}{Q'}\right)$,

(*e*) $P' \equiv P \pmod{Q}$ *implica* $\left(\frac{P'}{Q}\right) = \left(\frac{P}{Q}\right)$.

*Demostración.* En principio ($a$) es obvio a partir de la definición de $\left(\frac{P}{Q}\right)$ y ($b$) se deduce de la definición y del Teorema 3.1*b*. Entonces ($c$) se deduce de ($b$) y ($a$) y lo mismo acontece con ($d$). Para probar ($e$) se escribe $Q = q_1q_2 \cdots q_s$. Entonces $P' \equiv P \pmod{q_j}$ de modo que $\left(\frac{P'}{q_j}\right) = \left(\frac{P}{q_j}\right)$ por el Teorema 3.1*c* y entonces se concluye ($e$) *a* partir de la Definición 3.4.

**Teorema 3.6** *Si $Q$ es impar y $Q > 0$, entonces*

$$\left(\frac{-1}{Q}\right) = (-1)^{(Q-1)/2} \quad \text{y} \quad \left(\frac{2}{Q}\right) = (-1)^{(Q^2-1)/8}$$

*Demostración.* Se tiene

$$\left(\frac{-1}{Q}\right) = \prod_{j=1}^{s}\left(\frac{-1}{q_j}\right) = \prod_{j=1}^{s}(-1)^{(q_j-1)/2} = (-1)^{\sum_{j=1}^{s}(q_j-1)/2}$$

Si $a$ y $b$ son impares, entonces

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{(a-1)(b-1)}{2} \equiv 0 \pmod{2}$$

y de aquí que

$$\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \pmod{2}.$$

Aplicando esto repetidamente se obtiene

$$(3.1)\qquad \sum_{j=1}^{s}\frac{q_j-1}{2}\equiv\frac{1}{2}\left(\prod_{j=1}^{s}q_j-1\right)\equiv\frac{Q-1}{2}\pmod{2},$$

y así

$$\left(\frac{-1}{Q}\right)=(-1)^{(Q-1)/2}.$$

De modo semejante, si $a$ y $b$ son impares, entonces

$$\frac{a^2b^2-1}{8}-\left(\frac{a^2-1}{8}+\frac{b^2-1}{8}\right)=\frac{(a^2-1)(b^2-1)}{8}\equiv 0\pmod{8},$$

de modo que se tiene

$$\frac{a^2-1}{8}+\frac{b^2-1}{8}\equiv\frac{a^2b^2-1}{8}\pmod{2},$$

$$\sum_{j=1}^{s}\frac{q_j^2-1}{8}\equiv\frac{Q^2-1}{8}\pmod{2},$$

y de aquí que

$$\left(\frac{2}{Q}\right)=\prod_{j=1}^{s}\left(\frac{2}{q_j}\right)=(-1)^{\sum_{j=1}^{s}(q_j^2-1)/8}=(-1)^{(Q^2-1)/8}$$

**Teorema 3.7** *Si $P$ y $Q$ son impares y positivos y si $(P,Q)=1$, entonces*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right)=(-1)^{\{(P-1)/2\}\{(Q-1)/2\}}.$$

*Demostración.* Escribiendo $P=\prod_{i=1}^{r}p_i$ así como $Q=\prod_{j=1}^{s}q_j$ se tiene

$$\left(\frac{P}{Q}\right)=\prod_{j=1}^{s}\left(\frac{P}{q_j}\right)=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right)=\prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)(-1)^{\{(p_i-1)/2\}\{(q_j-1)/2\}}$$

$$=\left(\frac{Q}{P}\right)(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}}$$

donde se ha usado el Teorema 3.4. Pero

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\,\frac{q_j-1}{2}=\sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2}$$

y

$$\sum_{i=1}^{r} \frac{p_i - 1}{2} \equiv \frac{P-1}{2}, \qquad \sum_{j=1}^{s} \frac{q_j - 1}{2} \equiv \frac{Q-1}{2} \pmod 2$$

como en (3.1) en la demostración del Teorema 3.6. Por tanto se tiene

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)(-1)^{\{(P-1)/2\}\{(Q-1)/2\}}$$

lo cual demuestra el teorema.

El teorema que acaba de probarse demuestra que el símbolo de Jacobi obedece la ley de reciprocidad. Vale la pena considerar lo que se ha hecho. En este capítulo nos hemos interesado en los residuos cuadráticos. La definición del símbolo de Legendre es algo natural. A continuación se probó la célebre y útil ley de la reciprocidad para este símbolo. El símbolo de Jacobi es una extensión del símbolo de Legendre, definiendo $\left(\frac{P}{Q}\right)$ para $Q$ compuesto. Sin embargo, en principio podría haber parecido más natural definir $\left(\frac{P}{Q}\right)$ como 1 para los residuos cuadráticos $P$ y $-1$ para no residuos módulo $Q$. Si así se hubiera hecho, no se hubiera tenido ley de reciprocidad ($P = 5$, $Q = 9$ es un ejemplo). Lo que se hizo es esto: se renunció a la relación con los residuos cuadráticos en favor de la ley de reciprocidad. Esto no significa que el símbolo de Jacobi no pueda usarse en cálculos como los realizados en la Sección 3.2. De hecho, el símbolo de Jacobi juega un importante papel en tales cálculos. En la sección 3.2 se usa la ley de la reciprocidad para invertir el símbolo $\left(\frac{p}{q}\right)$ a $\left(\frac{q}{p}\right)$, pero podría hacerse solamente si $q$ fuera primo. Para calcular $\left(\frac{a}{p}\right)$ tuvo que factorizarse $a$ y considerar un producto de símbolos de Legendre. Sin embargo, usando ahora los símbolos de Jacobi no es necesario factorizar $a$ si es impar y positivo. Se calcula $\left(\frac{a}{p}\right)$ como un símbolo de Jacobi y entonces se sabe el carácter cuadrático de $a$ módulo $p$ si $p$ es primo.

Por ejemplo:

$$\left(\frac{105}{317}\right) = \left(\frac{317}{105}\right) = \left(\frac{2}{105}\right) = 1,$$

y de aquí que 105 es un residuo cuadrático módulo el primo 317.

**Problemas**

1. Evaluar: $\left(\frac{-23}{83}\right)$; $\left(\frac{51}{71}\right)$; $\left(\frac{71}{73}\right)$; $\left(\frac{-35}{97}\right)$.
2. ¿Cuáles de las siguientes congruencias pueden resolverse?
   ($a$) $x^2 \equiv 10 \pmod{127}$;
   ($b$) $x^2 \equiv 73 \pmod{173}$;
   ($c$) $x^2 \equiv 137 \pmod{401}$.
3. ¿Cuáles de las siguientes congruencias pueden resolverse?
   ($a$) $x^2 \equiv 11 \pmod{61}$; ($b$) $x^2 \equiv 42 \pmod{97}$;
   ($c$) $x^2 \equiv -43 \pmod{79}$; ($d$) $x^2 - 31 \equiv 0 \pmod{103}$.
4. Demostrar que si $p$ y $q$ son primos impares uno de los cuales es de la forma $4k + 1$, entonces $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$.
5. Probar que $\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0$, $p$ un primo impar.
6. Si $p$ es un primo impar y $(a, p) = 1$, probar que $ax^2 + bx + c \equiv 0 \pmod{p}$ tiene dos, una o ninguna solución de acuerdo con que $b^2 - 4ac$ sea un residuo cuadrático, congruente a cero o bien un no residuo cuadrático módulo $p$.
7. Usar el teorema de Wilson para probar que si $p$ es un primo de la forma $4n + 3$, entonces
$$1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} \equiv (-1)^m \pmod{p}$$
   donde $m$ es el número de no residuos cuadráticos entre los factores del primer miembro.
8. ($a$) Sea $p$ un primo impar con un residuo cuadrático $a$. Probar que $x^2 \equiv a \pmod{p^2}$ tiene exactamente dos soluciones, escribiendo $x = x_1 + py$ donde $x_1$ es una solución de $x^2 \equiv a \pmod{p}$.
   ($b$) Generalizar mediante el uso de inducción matemática y establecer que $x^2 \equiv a \pmod{p^k}$ tiene exactamente dos soluciones.
9. Sean $p_1, p_2, \cdots, p_n$ los divisores primos del entero impar $m$ y sea $(a, m) = 1$. Probar que $x^2 \equiv a \pmod{m}$ tiene una solución si y solamente si $\left(\frac{a}{p_i}\right) = 1$ para $i = 1, 2, \cdots, n$.
10. ¿Para cuáles primos $p$ existen los enteros $x$ y $y$ con $(x, p) = 1$, $(y, p) = 1$, tales que $x^2 + y^2 \equiv 0 \pmod{p}$?
11. ¿Para cuáles potencias primos $p^a$ existen los enteros $x$ y $y$ con $(x, p) = 1$, $(y, p) = 1$, tales que $x^2 + y^2 \equiv 0 \pmod{p^a}$?
12. ¿Para cuáles enteros positivos $n$ existen los enteros $x$ y $y$ con $(x, n) = 1$, $(y, n) = 1$, tales que $x^2 + y^2 \equiv 0 \pmod{n}$?
13. Sean los enteros $1, 2, \cdots, p - 1$ módulo $p$, $p$ un primo impar, divididos en dos conjuntos no vacíos $S_1$ y $S_2$ de modo que el producto de dos elementos del mismo conjunto está en $S_1$, mientras que el producto de un elemento de $S_1$ y un elemento de $S_2$ está en $S_2$. Probar que $S_1$ consiste de los residuos cuadráticos, $S_2$ de los no residuos, módulo $p$. *Sugerencia*: usar una raíz primitiva módulo $p$.

14. Sea $k$ impar. Probar que: si $a \geqq n$, entonces $x^2 \equiv 2^a k \pmod{2^n}$ tiene por lo menos una solución. Si $a < n$, entonces la congruencia tiene una solución si y solamente si $a$ es par y $x^2 \equiv k \pmod{2^{n-a}}$ tiene una solución.
15. Sea $k$ impar. Probar que $x^2 \equiv k \pmod 2$ tiene exactamente una solución. Además, $x^2 \equiv k \pmod{2^2}$ puede resolverse si y solamente si $k \equiv 1 \pmod 4$, en cuyo caso existen dos soluciones.
16. Sea $k$ impar y $n \geqq 3$. Probar que $x^2 \equiv k \pmod{2^n}$ puede resolverse si y solamente si $k \equiv 1 \pmod 8$. *Sugerencia*: aplicar la inducción matemática. Suponiendo que $x^2 \equiv k \pmod{2^n}$ tiene una solución $u$, demostrar que puede encontrarse un entero $t$ de modo que $(u + 2^{n-1}t)^2 \equiv k \pmod{2^{n+1}}$.
17. Supóngase que $n \geqq 3$ y $k \equiv 1 \pmod 8$. Probar que cualquier solución $u$ de $x^2 \equiv k \pmod{2^n}$ conduce a otras tres soluciones, $-u$, $u + 2^{n-1}$ y $-u + 2^{n-1}$. Probar que estas cuatro soluciones son incongruentes módulo $2^n$.
18. Probar que si $u$ y $v$ son números impares cualesquiera, entonces uno de $u - v$ y $u + v$ es de la forma $4m + 2$.
19. Sea $n \geqq 3$ y $k \equiv 1 \pmod 8$. Probar que si $u$ y $v$ son dos soluciones incongruentes de $x^2 \equiv k \pmod{2^n}$, entonces $v$ tiene una de las tres formas $-u, u + 2^{n-1}, -u + 2^{n-1}$ módulo $2^n$. De aquí que la congruencia tiene exactamente cuatro soluciones. *Sugerencia*: analizar $u^2 \equiv v^2 \pmod{2^n}$ y de aquí que $(u - v)(u + v) \equiv 0 \pmod{2^n}$, a la luz del problema anterior.
20. Considérese la congruencia $x^2 \equiv a \pmod{p^s}$ con $p$ primo, $s \geqq 1$, $a = p^t b$, $(b, p) = 1$. Probar que: si $t \geqq s$ la congruencia puede resolverse. Si $t < s$ la congruencia puede resolverse si y solamente si $t$ es par y $x^2 \equiv b \pmod{p^{s-t}}$ puede resolverse.
21. Considérese la congruencia $x^2 \equiv a \pmod m$. Para cada factor primo $p$ de $m$, denótese por $p^{s_p}$ la mayor potencia de $p$ que divide a $m$ y por $p^{t_p}$ la mayor potencia que divide a $a$, de modo que $s_p \geqq 1$, $t_p \geqq 0$. Escribir $c_p$ por $a/p^{t_p}$. Probar que la congruencia puede resolverse si y solamente si
    (1) para cada factor primo impar $p$ de $m$ tal que $t_p < s_p$, el entero $t_p$ es par y $\left(\frac{c_p}{p}\right) = 1$;
    (2) en caso de que $m$ sea par y $t_2 < s_2$, entonces $t_2$ es par y $c_2 \equiv 1 \pmod{2^r}$ donde $r = \min(3, s_2 - t_2)$.
22. Sea $p$ cualquier primo impar. Denotemos por $f(a)$ el número de soluciones $x, y$ de $x^2 - y^2 \equiv a \pmod p$, donde dos soluciones $x_1, y_1$, y $x_2, y_2$, se consideran separadamente a menos que $x_1 \equiv x_2$ y $y_1 \equiv y_2 \pmod p$. Probar que $f(a) = p - 1$ a menos que $p|a$, en cuyo caso el resultado es $f(a) = 2p - 1$.

Para los siguientes problemas extenderemos el alcance del significado del símbolo $\left(\frac{a}{p}\right)$ definiéndolo como 0 siempre que $p|a$.

23. Probar que

$$\sum_{m=1}^{p} \left(\frac{am + b}{p}\right) = 0,$$

suponiendo que $a \not\equiv 0 \pmod p$. También probar que $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ y que $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ si $a \equiv b \pmod p$.

24. Considérese la sucesión $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \cdots, \left(\frac{p-1}{p}\right)$, para cualquier primo impar $p$. Cualquier par consecutivo de términos de la sucesión es de uno de los cuatro tipos, 1, 1 o bien $-1$, $-1$ o bien 1, $-1$, o bien $-1$, 1. Denotemos el número de ocurrencias de cada uno de estos tipos por $N(1,1)$, $N(-1,-1)$, $N(1,-1)$ y $N(-1,1)$, respectivamente. Probar que

$$2N(1,1) - 2N(-1,-1) = \sum_{x=1}^{p-2} \left\{\left(\frac{x}{p}\right) + \left(\frac{x+1}{p}\right)\right\},$$

$$2N(1,-1) - 2N(-1,1) = \sum_{x=1}^{p-2} \left\{\left(\frac{x}{p}\right) - \left(\frac{x+1}{p}\right)\right\}.$$

25. Probar que $\sum_{x=1}^{p} \left(\frac{x}{p}\right)\left(\frac{x+1}{p}\right) = -1$ si $p$ es cualquier primo impar. *Sugerencia*: definir $s(a,p) = \sum_{x=1}^{p} \left(\frac{x}{p}\right)\left(\frac{x+a}{p}\right)$ y probar que $s(a,p) = s(1,p)$ si $p \nmid a$. Entonces evaluar $\sum_{a=1}^{p-1} s(a,p)$.

26. Usando la notación de los dos problemas precedentes demostrar que $-s(1,p)$ es el exceso del número de cambios de signo en la sucesión $\left(\frac{1}{p}\right), \left(\frac{2}{p}\right), \cdots, \left(\frac{p-1}{p}\right)$ sobre el número de veces en que el signo no cambia.
De aquí probar que

$$N(1,-1) + N(-1,1) - N(1,1) - N(-1,-1) = +1.$$

Entonces establecer en el caso de que $p \equiv 1 \pmod 4$ que

$$N(1,1) + 1 = N(1,-1) = N(-1,1) = N(-,-1) = (p-1)/4,$$

y en el caso de que $p \equiv 3 \pmod 4$ que

$$N(1,-1) - 1 = N(1,1) = N(-1,1) = N(-1,-1) = (p-3)/4,$$

27. Probar que si $p$ es un primo impar entonces $\sum_{m=1}^{p} \left(\frac{m^2-b}{p}\right) = -1$ a menos que $p|b$, en cuyo caso la suma tiene el valor $p-1$.

Capitulo 4

# Algunas funciones de la teoría de los números

## 4.1 Función máximo entero

La función $[x]$ se introdujo en la Definición 3.3. Se define para todo $x$ real y solamente asume valores enteros. Muchas de sus propiedades se incluyen en el siguiente teorema.

**Teorema 4.1** *Sea $x$ y $y$ números reales. Entonces se tiene*

*a*) $[x] \leqq x < [x] + 1,\ x - 1 < [x] \leqq x,\ 0 \leqq x - [x] < 1.$

*b*) $[x] = \sum_{1 \leqq i \leqq x} 1$ si $x \geqq 0.$

*c*) $[x + m] = [x] + m$ *si* $m$ *es un entero.*

*d*) $[x] + [y] \leqq [x + y] \leqq [x] + [y] + 1.$

*e*) $[x] + [-x] = \begin{cases} 0 & \text{si } x \text{ es un entero,} \\ -1 & \text{en cualquier otro caso.} \end{cases}$

*f*) $\left[\dfrac{[x]}{m}\right] = \left[\dfrac{x}{m}\right]$ *si* $m$ *es un entero positivo.*

*g*) $x - [x]$ *es la parte fraccionaria de* $x$.

*h*) $-[-x]$ *es el menor entero* $\geqq x$.

*i*) $[x + \frac{1}{2}]$ *es el entero más próximo a* $x$. *Si dos enteros son igualmente próximos a* $x$, *es el mayor de los dos.*

*j*) $-[-x + \frac{1}{2}]$ *es el entero más próximo a* $x$. *Si dos enteros son igualmente próximos a* $x$, *es el menor de los dos.*

*Demostración.* La primera parte de $(a)$ es precisamente la definición de $[x]$ en su forma algebraica. Las otras dos partes son rearreglos de la primera parte.

En $(b)$ la suma es vacía si $x < 1$. Adoptemos la convención de que una suma vacía es cero. Entonces, para $x \geqq 0$, la suma considera el número de enteros positivos $i$ que sean menores que ó iguales a $x$. Este número evidentemente es $[x]$

La parte $(c)$ es obvia a partir de la definición de $[x]$.

Para probar $(d)$ se escribe $x = n + \nu$, $y = m + \mu$, donde $m$ y $n$ son enteros y $0 \leqq \nu < 1$, $0 \leqq \mu < 1$. Entonces

$$[x] + [y] = n + m \leqq [n + \nu + m + \mu]$$
$$= n + m + [\nu + \mu] \leqq n + m + 1 = [x] + [y] + 1.$$

Una vez más, escribiendo $x = n + \nu$, también se tiene $-x = -n - 1 + 1 - \nu$, $0 < 1 - \nu \leqq 1$. Entonces

$$[x] + [-x] = n + [-n - 1 + 1 - \nu]$$
$$= n - n - 1 + [1 - \nu] = \begin{cases} 0 & \text{si } \nu = 0 \\ -1 & \text{si } \nu > 0, \end{cases}$$

y se tiene $(e)$.

Para probar $(f)$ se escribe $x = n + \nu$, $n = qm + r$, $0 \leqq \nu < 1$, $0 \leqq r \leqq m - 1$ y se tiene

$$\left[\frac{x}{m}\right] = \left[\frac{qm + r + \nu}{m}\right] = q + \left[\frac{r + \nu}{m}\right] = q,$$

dado que $0 \leqq r + \nu < m$. Entonces se deduce $(f)$ debido a que

$$\left[\frac{[x]}{m}\right] = \left[\frac{n}{m}\right] = \left[q + \frac{r}{m}\right] = q.$$

La parte $(g)$ es nada más que una definición de las palabras "parte fraccionaria de $x$".

Reemplazando $x$ por $-x$ en $(a)$ se obtiene $-x - 1 < [-x] \leqq -x$ y de aquí que $x \leqq -[-x] < x + 1$, lo cual prueba $(h)$.

Para probar $(i)$ sea $n$ el entero más próximo a $x$, tomando el mayor si los dos son igualmente distantes. Entonces $n = x + \theta$, $-\frac{1}{2} < \theta \leqq \frac{1}{2}$, y $[x + \frac{1}{2}] = n + [-\theta + \frac{1}{2}] = n$ puesto que $0 \leqq -\theta + \frac{1}{2} < 1$.

La demostración de $(j)$ es semejante a la de $(i)$.

**Teorema 4.2** *Supóngase que $p$ denota un primo. Entonces el mayor exponente $e$ tal que $p^e | n!$ es*

$$e = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

*Demostración.* Si $p^i > n$, entonces $[n/p^i] = 0$. Por lo tanto la suma termina, no es realmente una serie infinita. El teorema se demuestra

fácilmente por inducción matemática. Es verdadero para 1!. Supóngase que es verdadero para $(n-1)!$ y denotemos por $j$ el mayor entero tal que $p^j|n$. Dado que $n! = n \cdot (n-1)!$, debemos probar que $\sum [n/p^i] - \sum [(n-1)/p^i] = j$. Pero

$$\left[\frac{n}{p^i}\right] - \left[\frac{n-1}{p^i}\right] = \begin{cases} 1 \text{ si } p^i|n \\ 0 \text{ si } p^i \nmid n \end{cases}$$

y de aquí que
$$\sum \left[\frac{n}{p^i}\right] - \sum \left[\frac{n-1}{p^i}\right] = j.$$

La demostración precedente es corta pero un tanto artificial. Puede basarse una demostración diferente en una observación sencilla pero interesante. Si $a_1, a_2, \ldots, a_n$ son enteros no negativos, denotemos por $f(1)$ el número de ellos que son mayores que o iguales a 1, por $f(2)$ el número de mayores que o iguales a 2, etc. Entonces

$$a_1 + a_2 + \cdots + a_n = f(1) + f(2) + f(3) + \cdots.$$

Ahora bien, para $1 \leqq j \leqq n$, sea $a_j$ el máximo entero tal que $p^{a_j}|j$. Entonces $f(1)$ considera el número de enteros $\leqq n$ que son divisibles entre $p$, $f(2)$ el número de los divisibles entre $p^2$, etc. De aquí que $f(k)$ considera los enteros $p^k, 2p^k, 3p^k, \ldots, [n/p^k]p^k$, de manera que $f(k) = [n/p^k]$. De donde se ve que

$$e = a_1 + a_2 + \cdots + a_n = \sum_{i=1}^{\infty} f(i) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right].$$

La fórmula ($f$) del Teorema 4.1 acorta el trabajo requerido para calcular $e$ en el Teorema 4.2. Por ejemplo, si se desea encontrar la máxima potencia de 7 que divide a 1000! se calcula

$$[1000/7] = 142, [142/7] = 20, [20/7] = 2, [2/7] = 0.$$

Sumando se encuentra que $7^{164}|1000!$, $7^{165} \nmid 1000!$.

Las aplicaciones del Teorema 4.2 no se restringen a los problemas numéricos. Como un ejemplo, probemos que

$$\frac{n!}{a_1!a_2! \cdots a_r!}$$

es un entero si $a_i \geqq 0$, $a_1 + a_2 + \cdots + a_r = n$. Para hacerlo simplemente debe demostrarse que todo primo divide al numerador para, por lo menos, la potencia más alta que divide al denominador. Aplicando el Teorema 4.2 solamente es necesario probar que

$$\sum \left[\frac{n}{p^i}\right] \geqq \sum \left[\frac{a_1}{p^i}\right] + \sum \left[\frac{a_2}{p^i}\right] + \cdots + \sum \left[\frac{a_r}{p^i}\right].$$

Pero la aplicación repetida del Teorema 4.1*d* nos da

$$\left[\frac{a_1}{p^i}\right] + \left[\frac{a_2}{p^i}\right] + \cdots + \left[\frac{a_r}{p^i}\right] \leqq \left[\frac{a_1 + a_2 + \cdots + a_r}{p^i}\right] = \left[\frac{n}{p^i}\right]$$

Sumando esta expresión sobre $i$ se tiene el resultado deseado.

Un ejemplo ligeramente más complicado es probar que

$$\frac{(ab)!}{a!(b!)^a}$$

es un entero. Debe demostrarse que

$$\sum \left[\frac{ab}{p^i}\right] - \sum \left[\frac{a}{p^i}\right] - a \sum \left[\frac{b}{p^i}\right] \geqq 0$$

para todo primo $p$. Denotemos por $r$ y $s$ los enteros tales que $p^r \leqq a < p^{r+1}$ y $p^s \leqq b < p^{s+1}$. Entonces

$$\sum \left[\frac{ab}{p^i}\right] - \sum \left[\frac{a}{p^i}\right] - a \sum \left[\frac{b}{p^i}\right]$$

$$= \sum_{i=1}^{s} \left[\frac{ab}{p^i}\right] + \sum_{i=s+1}^{r+s} \left[\frac{ab}{p^i}\right] + \sum_{i=r+s+1}^{\infty} \left[\frac{ab}{p^i}\right] - \sum_{i=1}^{r} \left[\frac{a}{p^i}\right] - \sum_{i=1}^{s} a \left[\frac{b}{p^i}\right]$$

$$= \sum_{i=1}^{s} \left(\left[\frac{ab}{p^i}\right] - a \left[\frac{b}{p^i}\right]\right) + \sum_{i=1}^{r} \left(\left[\frac{ab}{p^{s+i}}\right] - \left[\frac{a}{p^i}\right]\right) + \sum_{i=r+s+1}^{\infty} \left[\frac{ab}{p^i}\right]$$

$$\geqq \sum_{i=1}^{s} \left(\left[\frac{ab}{p^i}\right] - a \left[\frac{b}{p^i}\right]\right) + \sum_{i=1}^{r} \left(\left[\frac{ap^s}{p^{s+i}}\right] - \left[\frac{a}{p^i}\right]\right)$$

$$= \sum_{i=1}^{s} \left(\left[\frac{ab}{p^i}\right] - a \left[\frac{b}{p^i}\right]\right) \geqq 0$$

dado que, por aplicación repetida del Teorema 4.1*d*, $[ab/p^i] \geqq a[b/p^i]$.

**Problemas**

1. ¿Cuál es la mayor potencia de 2 que divide a 533!? ¿La mayor potencia de 3? ¿La mayor potencia de 6? ¿La mayor potencia de 12? ¿La mayor potencia de 70?
2. Si se escribiera 100! en la notación decimal ordinaria sin el signo factorial, ¿cuántos ceros se escribirían en línea en el extremo derecho?

3. ¿Para qué números reales $x$ es verdad que
   a) $[x] + [x] = [2x]$;
   b) $[x + 3] = 3 + [x]$;
   c) $[x + 3] = 3 + x$;
   d) $[x + \frac{1}{2}] + [x - \frac{1}{2}] = [2x]$;
   e) $[9x] = 9$?
4. Dado que $[x + y] = [x] + [y]$ y $[-x - y] = [-x] + [-y]$, probar que $x$ o bien $y$ es un entero.
5. Encontrar las fórmulas para los exponentes máximos $e$ del primo $p$ tales que $p^e$ divide a $(a)$ el producto $2 \cdot 4 \cdot 6 \cdots (2n)$ de los primeros $n$ números pares; $(b)$el producto de los primeros $n$ números impares.
6. Para cualquier número real $x$ probar que $[x] + [x + \frac{1}{2}] = [2x]$.
7. Para números reales positivos cualesquiera $x$ y $y$ probar que $[x] \cdot [y] \leqq [xy]$.
8. Para números reales positivos cualesquiera $x$ y $y$ probar que

$$[x - y] \leqq [x] - [y] \leqq [x - y] + 1.$$

9. Probar que $(2n)!/(n!)^2$ es par si $n$ es un entero positivo.
10. Sea $m$ cualquier número real no cero o bien un entero positivo. Probar que existe un $x$ tal que la ecuación del Teorema 4.1$f$ es falsa.
11. Si $p$ y $q$ son primos distintos, probar que los divisores de $p^2q^3$ coinciden con los términos de $(1 + p + p^2)(1 + q + q^2 + q^3)$ cuando estos últimos se multiplican.
12. Probar que $\prod_{i=1}^{n} (a + i)$ es divisible entre $n!$.
13. Si $a$ y $b$ son enteros tales que $(a, b) = 1$ y $\rho$ es un número real tal que $a\rho$ y $b\rho$ son enteros, entonces $\rho$ es un entero. De aquí probar que $\rho = n!/(a!b!)$ es un entero si $(a, b) = 1$ y $a + b = n + 1$. Generalizar esto para probar que

$$\rho = \frac{n!}{a_1!a_2! \cdots a_r!}$$

es un entero si $(a_1, a_2, \cdots, a_r) = 1$ y $a_1 + a_2 + \cdots + a_r = n + 1$.
14. Considérese un entero $n \geqq 1$ y los enteros $i$, $1 \leqq i \leqq n$. Para cada $k = 0, 1, 2, \cdots$ encontrar el número de $i$-es que son divisibles entre $2^k$ pero no entre $2^{k+1}$. Así probar que

$$\sum_{j=1}^{\infty} \left[\frac{n}{2^j} + \frac{1}{2}\right] = n,$$

y de aquí que se obtiene el valor correcto de la suma $n/2 + n/4 + n/8 + \cdots$ si se reemplaza cada término por su entero más próximo, usando el mayor si existen dos.
15. Si $n$ es cualquier entero positivo y $\xi$ cualquier número real, probar que

$$[\xi] + \left[\xi + \frac{1}{n}\right] + \cdots + \left[\xi + \frac{n-1}{n}\right] = [n\xi].$$

16. Probar que un número $\alpha$ es racional si y solamente si existe un entero positivo $k$ tal que $[k\alpha] = k\alpha$. Probar que un número $\alpha$ es racional si y solamente si existe un entero positivo $k$ tal que $[(k!)\alpha] = (k!)\alpha$.

17. Recordando que la constante matemática $e$ tiene el valor $\sum_{j=0}^{\infty} 1/j!$, probar que

$$[(k!)e] = k! \sum_{j=0}^{k} 1/j! < (k!)e.$$

De aquí probar que $e$ es irracional.

18. Si $(m, n) = 1$, probar que

$$\sum_{x=1}^{n-1} \left[\frac{mx}{n}\right] = \frac{(m-1)(n-1)}{2}.$$

19. Si $m \geqq 1$, probar que $[(1+\sqrt{3})^{2m+1}]$ es divisible entre $2^{m+1}$ pero no entre $2^{m+2}$.

20. Sea $\theta$ irracional y $0 < \theta < 1$. Definir

$$g_n = \begin{cases} 0 \text{ si } [n\theta] = [(n-1)\theta], \\ 1 \text{ en cualquier otro caso.} \end{cases}$$

Probar que $$\lim_{n\to\infty} \frac{g_1 + g_2 + \cdots + g_n}{n} = \theta.$$

21. Sea $n$ un entero impar $> 5$. Si $n$ se factoriza en el producto de dos enteros, $n = uv$, con $u > v$ y $u - v \leqq \sqrt[4]{64n}$, probar que las raíces de $x^2 - 2[\sqrt{n} + 1]x + n = 0$ son enteros. *Sugerencia:* usar la identidad $\{(u+v)/2\}^2 - \{(u-v)/2\}^2 = uv$ para obtener cotas sobre el entero $(u+v)/2$.

22. Sea $\alpha$ un número irracional positivo. Probar que las dos sucesiones

$[1+\alpha], [2+2\alpha], \cdots, [n+n\alpha], \cdots,$ y

$[1+\alpha^{-1}], [2+2\alpha^{-1}], \cdots, [n+n\alpha^{-1}], \cdots,$

juntas contienen a todo entero positivo exactamente una vez. Probar que esto es falso si $\alpha$ es racional.

23. Sea $S$ el conjunto de enteros dados por $[\alpha x]$ y $[\beta x]$ para $x = 1, 2, \cdots$. Probar que $S$ consiste de todo entero positivo, apareciendo cada uno exactamente una vez, si y solamente si $\alpha$ y $\beta$ son números irracionales positivos tales que $\dfrac{1}{\alpha} + \dfrac{1}{\beta} = 1$.

24. Para los números reales positivos $\alpha, \beta, \gamma$ definir $f(\alpha, \beta, \gamma)$ como la suma de todos los términos positivos de la serie

$$\left[\frac{\gamma-\alpha}{\beta}\right] + \left[\frac{\gamma-2\alpha}{\beta}\right] + \left[\frac{\gamma-3\alpha}{\beta}\right] + \left[\frac{\gamma-4\alpha}{\beta}\right] + \cdots.$$

(Si no existen términos positivos, definir $f(\alpha, \beta, \gamma) = 0$). Probar que $f(\alpha, \beta, \gamma) = f(\beta, \alpha, \gamma)$. *Sugerencia:* $f(\alpha, \beta, \gamma)$ está relacionada al número de soluciones de $\alpha x + \beta y \leqq \gamma$ en los pares de enteros no negativos $x$, $y$.

25. Probar que si $p$ es un primo y $0 \leqq n \leqq p^k$ entonces

$$\binom{p^k}{n} \equiv \begin{cases} 1 \pmod{p} \text{ si } n = 0 \text{ ó } p^k, \\ 0 \pmod{p} \text{ si } 1 \leqq n \leqq p^k - 1, \end{cases}$$

donde $\binom{p^k}{n}$ es el coeficiente binomial.

26. Probar que si $p$ es un primo y $0 \leqq n \leqq p^k$ entonces

$$\binom{p^k}{n} \equiv \begin{cases} 1 \pmod{p^2} \text{ si } n = 0 \text{ o bien } p^k, \\ pa'(-1)^{a-1} \pmod{p^2} \text{ si } n = ap^{k-1}, 1 \leqq a \leqq p-1, & aa' \equiv 1 \pmod{p}, \\ 0 \pmod{p^2} \text{ en cualquier otro caso} \end{cases}$$

27. Probar que si $p$ es un primo y $m = \sum_{j=0}^{r} a_j p^j$, $n = \sum_{j=0}^{r} b_j p^j$, $0 \leqq a^j \leqq p - 1$, $0 \leqq b_j \leqq p - 1$, entonces

$$\binom{m}{n} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1}\binom{a_2}{b_2} \cdots \binom{a_r}{b_r} \pmod{p}.$$

*Sugerencia:* considérese $(1 + x)^m \pmod{p}$.

## 4.2 Funciones numéricas

Las funciones, tales como la $\phi(m)$ del Teorema 2.5, que están definidas para los valores enteros positivos de su argumento reciben el nombre de funciones numéricas.

**Definición 4.1** *Para los enteros positivos $n$ se hacen las definiciones siguientes.*

$\tau(n)$ *es el número de divisores positivos de $n$.*

$\sigma(n)$ *es la suma de los divisores positivos de $n$.*

$\sigma_k(n)$ *es la suma de las $k$-ésimas potencias de los divisores positivos de $n$.*

Por ejemplo, $\tau(6) = 4$, $\sigma(6) = 12$, $\sigma_2(6) = 50$. Estas son todas las funciones numéricas. El valor de $k$ puede ser cualquier número real, positivo, negativo o cero. Las funciones $\tau(n)$ y $\sigma(n)$ son simplemente casos especiales de $\sigma_k(n)$, puesto que $\tau(n) = \sigma_0(n)$, $\sigma(n) = \sigma_1(n)$. Es conveniente usar los símbolos $\sum_{d|n} f(d)$ y $\prod_{d|n} f(d)$ para la suma y el producto de $f(d)$ sobre todos los divisores positivos $d$ de $n$. Por lo tanto, se escribe

$$\tau(n) = \sum_{d|n} 1, \quad \sigma(n) = \sum_{d|n} d, \quad \sigma_k(n) = \sum_{d|n} d^k.$$

**Teorema 4.3** *Si $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ entonces* $\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$. *También* $\tau(1) = 1$.

*Demostración.* Un entero positivo $d$ divide a $n$ si, y solamente si, $d = p_1^{f_1}p_2^{f_2} \cdots p_r^{f_r}$ con $0 \leqq f_i \leqq e_i$ para $i = 1, 2, \cdots, r$. De donde existen precisamente $(e_1 + 1)(e_2 + 1) \cdots (e_r + 1)$ de tales $d$.

Si $(m, n) = 1$ se deduce, con base en el Teorema 4.3, que $\tau(mn) = \tau(m)\tau(n)$.

**Definición 4.2** *Si $f(n)$ es una función numérica tal que $f(mn) = f(m)f(n)$ para toda pareja $m, n$ que satisfaga $(m, n) = 1$, entonces se dice que $f(n)$ es multiplicativa. Si $f(m, n) = f(m)f(n)$ ya sea que $m$ y $n$ sean relativamente primos o no, se dice que $f(n)$ es totalmente multiplicativa.*

**Teorema 4.4** *Sea $f(n)$ una función multiplicativa y $F(n) = \sum_{d|n} f(d)$. Entonces $F(n)$ es multiplicativa.*

*Demostración.* Supóngase que $(m, n) = 1$. Entonces $m$ y $n$ tienen representaciones canónicas

$$n = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \qquad m = q_1^{\beta_1}q_2^{\beta_2} \cdots q_s^{\beta_s},$$

con exponentes positivos $\alpha_i$ y $\beta_i$ y donde $p_1, p_2, \cdots, p_r, q_1, q_2, \cdots, q_s$ son primos distintos. Los divisores positivos $d_1$ de $n$ son precisamente los números $d_1 = p_1^{\gamma_1}p_2^{\gamma_2} \cdots p_r^{\gamma_r}$ para todas las selecciones posibles de los $\gamma$ que satisfagan $0 \leqq \gamma_i \leqq \alpha_i$. De modo semejante, los divisores positivos $d_2$ de $m$ están dados por $d_2 = q_1^{\delta_1}q_2^{\delta_2} \cdots q_s^{\delta_s}$, $0 \leqq \delta_i \leqq \beta_i$ Por lo tanto, conforme $d_1$ recorre todos los divisores positivos de $n$ y $d_2$ recorre todos los divisores positivos de $m$, su producto $d_1d_2$ recorre los valores $d = d_1d_2 = p_1^{\gamma_1}p_2^{\gamma_2} \cdots p_r^{\gamma_r}q_1^{\delta_1}q_2^{\delta_2} \cdots q_s^{\delta_s}$, $0 \leqq \gamma_i \leqq \alpha$, $0 \leqq \delta \leqq \beta$; pero éstos son precisamente todos los divisores positivos de $nm = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r} q_1^{\beta_1}q_2^{\beta_2} \cdots q_s^{\beta_s}$. En otras palabras.

$$\sum_{d_1|n} \sum_{d_2|m} f(d_1d_2) = \sum_{d|nm} f(d).$$

Es evidente que $(d_1, d_2) = 1$ y de aquí que se tiene

$$F(nm) = \sum_{d|nm} f(d) = \sum_{d_1|n} \sum_{d_2|m} f(d_1d_2) = \sum_{d_1|n} \sum_{d_2|m} f(d_1)f(d_2)$$

$$= \sum_{d_1|n} f(d_1) \sum_{d_2|m} f(d_2) = F(n)F(m).$$

Podría haberse usado este teorema y la Definición 4.1 para probar que $\tau(n)$ es multiplicativa. Puesto que $\tau(n) = \sum_{d|n} 1$ es de la forma $\sum_{d|n} f(d)$ y dado que la función $f(n) = 1$ es multiplicativa, puede aplicarse el

Teorema 4.4 y se ve que $\tau(n)$ es multiplicativa. Entonces hubiera sido fácil probar el Teorema 4.3. Si $p_i$ es un primo, entonces $\tau(p_i^{e_i}) = e_i + 1$, puesto que $p_i^{e_i}$ tiene los $e_i + 1$ divisores positivos $1, p_i, p_i^2 \cdots, p_i^{e_i}$ y no más. Entonces, dado que $\tau(n)$ es multiplicativa, se tiene

$$\begin{aligned}\tau(p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}) &= \tau(p_1^{e_1})\tau(p_2^{e_2})\cdots\tau(p_r^{e_r})\\ &= (e_1+1)(e_2+1)\cdots(e_r+1).\end{aligned}$$

Esto ejemplifica un método útil para manejar ciertas funciones numéricas. Se usará para encontrar una fórmula para $\sigma(n)$ en el siguiente teorema. Sin embargo debe puntualizarse que $\sigma(n)$ también puede encontrarse de manera más sencilla, en la misma forma como se obtuvo la primera fórmula para $\tau(n)$.

**Teorema 4.5** *Si* $n = p_1^{e_1}p_2^{e_2}\cdots, p_r^{e_r}$, *entonces*

$$\sigma(n) = \prod_{i=1}^{r}\frac{p_i^{e_i+1}-1}{p_i-1}, \qquad \sigma(1) = 1.$$

*Demostración.* Por definición, $\sigma(n) = \sum_{d|n} d$ de modo que puede aplicarse el Teorema 4.4 con $f(n) = n$, $F(n) = \sigma(n)$. Así que $\sigma(n)$ es multiplicativa y $\sigma(n) = \prod_{i=1}^{n}\sigma(p_i^{e_i})$. Pero los divisores positivos de $p_i^{e_i}$ son precisamente $1, p_i\ p_i^2, \cdots, p_i^{e_i}$ cuya suma es $(p_i^{e_i+1}-1)/(p_i-1)$.

**Problemas**

1. Encontrar el menor entero $x$ para el cual $\phi(x) = 6$.
2. Encontrar el menor entero $x$ para el cual $\tau(x) = 6$.
3. Encontrar el menor entero positivo $n$ de manera que $\sigma(x) = n$ no tenga soluciones; exactamente una solución, exactamente dos soluciones, exactamente tres soluciones.
4. Encontrar el menor entero positivo $m$ para el cual existe otro entero positivo $n \neq m$ tal que $\sigma(m) = \sigma(n)$.
5. Probar que $\prod_{d|n} d = n^{\tau(n)/2}$.
6. Probar que $\sum_{d|n} d = \sum_{d|n} n/d$ y más generalmente que $\sum_{d|n} f(d) = \sum_{d|n} f(n/d)$.
7. Probar que $\sigma_{-k}(n) = n^{-k}\sigma_k(n)$.
8. Encontrar una fórmula para $\sigma_k(n)$.
9. Si $f(n)$ y $g(n)$ son funciones multiplicativas y $g(n) \neq 0$ para todo $n$, demostrar que las funciones $F(n) = f(n)g(n)$ y $G(n) = f(n)g(n)$ también son multiplicativas.

10. Dar un ejemplo para mostrar que si $f(n)$ es totalmente multiplicativa, $F(n)$ no necesita también ser totalmente multiplicativa, donde $F(n)$ se define como $\sum_{d|n} f(d)$.
11. Probar que el número de fracciones positivas irreducibles $\leqq 1$ con denominador $\leqq n$ es $\phi(1) + \phi(2) + \phi(3) + \cdots + \phi(n)$.
12. Probar que el número de divisores de $n$ es impar si y solamente si $n$ es un cuadrado perfecto. Si $k \geqq 1$, probar que $\sigma_k(n)$ es impar si y solamente si $n$ es un cuadrado o bien el doble de un cuadrado.
13. Dado cualquier entero positivo $n > 1$, probar que existe un número infinito de enteros $x$ que satisfacen $\tau(x) = n$.
14. Dado cualquier entero positivo $n$, probar que existe solamente un número finito de enteros $x$ que satisfacen $\phi(x) = n$; de modo semejante para $\sigma(x) = n$.
15. Probar que si $(a, b) > 1$ entonces $\sigma_k(ab) < \sigma_k(a)\sigma_k(b)$ y $\tau(ab) < \tau(a)$ $\tau(b)$.
16. Se dice (emulando a Euclides) que $m$ es un número perfecto si $\sigma(m) = 2m$, esto es, si $m$ es la suma de todos sus divisores positivos diferentes a sí mismo. Si $2^n - 1$ es un primo $p$, probar que $2^{n-1}p$ es un número perfecto. Usese este resultado para encontrar tres números perfectos.
17. Probar que un entero $q$ es primo si y solamente si $\sigma(q) = q + 1$.
18. Demostrar que si $\sigma(q) = q + k$ donde $k|q$ y $k < q$, entonces $k = 1$.
19. Probar que todo número perfecto par tiene la forma dado en el Problema 16. *Sugerencia*: Supóngase que $2^{n-1}q$ es un número perfecto, donde $n > 1$ y $q$ es impar. Escribir $\sigma(q) = q + k$ y así deducir, a partir de $\sigma(2^{n-1}q) = 2^n q$ que $q = k(2^n - 1)$. Por tanto, $k|q$ y $k < q$.
20. Para cualquier entero $n \geqq 2$ definir $\nu(n)$ como $(-1)^j$, donde $j$ es el número total de factores primos de $n$. Por ejemplo, si $n = 16$, entonces $j = 4$; si $n = 72$, $j = 5$. También definir $\nu(1) = 1$. Probar que $\nu(n)$ es una función totalmente multiplicativa y que

$$\sum_{d|n} \nu(d) = \begin{cases} 1 \text{ si } n \text{ es un cuadrado perfecto,} \\ 0 \text{ en cualquier otro caso} \end{cases}$$

21. Si $d|n$ y $\delta|(n/d)$, entonces $d|(n/\delta)$. Probar que el conjunto de parejas ordenadas $(d, \delta)$ donde $d$ recorre todos los divisores positivos de un entero fijo $n$ y, para cada valor de $d$, $\delta$ recorre todos los divisores positivos de $n/d$, es un conjunto simétrico en el sentido de que si $(a, b)$ está en el conjunto, también está $(b, a)$.
22. Probar que el cojunto de parejas del problema anterior es el mismo que el conjunto de parejas $(d, \delta)$ sobre todo positivo $d$ y $\delta$ tales que $d\delta|n$.
23. Considérese el conjunto de parejas ordenadas $(d, \gamma)$ donde $d$ recorre todos los divisores positivos de un entero fijo $n$ y, para cada una de esas $d$, $\gamma$ recorre todos los divisores positivos de $d$. Probar que éste es el mismo que el conjunto de parejas ordenadas $(\beta\gamma, \gamma)$ donde $\gamma$ recorre todos los divisores de $n$ y, para cada una de esas $\gamma$, $\beta$ recorre los divisores positivos de $n/\gamma$.

## 4.3 La fórmula de inversión de Moebius

**Definición 4.3** *La función de Moebius* $\mu(n)$ *se define por*

$$\mu(n) = \begin{cases} 1 & si\ n = 1 \\ 0 & si\ a^2|n\ para\ algún\ a > 1 \\ (-1)^r & si\ n = p_1p_2 \cdots p_r, p_i\ primos\ distintos. \end{cases}$$

**Teorema 4.6** *La función $\mu(n)$ es multiplicativa y*

$$\sum_{d|n} \mu(d) = \begin{cases} 1\ si\ n = 1 \\ 0\ si\ n > 1. \end{cases}$$

*Demostración.* Es evidente, a partir de la definición, que $\mu(n)$ es multiplicativa. Si $F(n) = \sum_{d|n} \mu(d)$, entonces $F(n)$, por el Teorema 4.4, es multiplicativa. Dado que $F(1) = \mu(1) = 1$ y $F(p^e) = \sum_{f=0}^{e} \mu(p^f) = 1 + (-1) = 0$, se tiene el resultado deseado.

**Teorema 4.7** *Fórmula de inversión de Moebius. Si $F(n) = \sum_{d|n} f(d)$ para todo entero positivo n, entonces $f(n) = \sum_{d|n} \mu(d)F(n/d)$.*

*Demostración.* Se tiene

$$\sum_{d|n} \mu(d)F\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \sum_{\delta|(n/d)} f(\delta) = \sum_{\delta|n} \sum_{d|(n/\delta)} \mu(d)f(\delta)$$

$$= \sum_{\delta|n} f(\delta) \sum_{d|(n/\delta)} \mu(d) = f(n)$$

por el Teorema 4.6

**Teorema 4.8** *Si $f(n) = \sum_{d|n} \mu(d)F(n/d)$ para todo entero positivo n, entonces $F(n) = \sum_{d|n} f(d)$.*

*Demostración.* Una vez más, por el Teorema 4.6 se encuentra

$$\sum_{d|n} f(d) = \sum_{d|n} \sum_{\delta|d} \mu(\delta)F\left(\frac{d}{\delta}\right) = \sum_{d|n} \sum_{\gamma|d} \mu\left(\frac{d}{\gamma}\right)F(\gamma)$$

$$= \sum_{\gamma|n} \sum_{\beta\gamma|n} \mu\left(\frac{\beta\gamma}{\gamma}\right)F(\gamma) = \sum_{\gamma|n} F(\gamma) \sum_{\beta|(n/\gamma)} \mu(\beta)$$

$$= F(n).$$

Debe hacerse notar que el Teorema 4.7 y su inverso, el Teorema 4.8, no requiere que $f(n)$ o bien $F(n)$ sean multiplicativas.

Los dos últimos teoremas frecuentemente son muy útiles. Como un ejemplo, se obtendrán los resultados de la Sección 2.4, referente a la función $\phi$ de Euler, en una forma diferente. En el Teorema 2.5 se vio que $\phi(n)$ es el número de enteros positivos menores que o iguales a $n$ que son

relativamente primos para $n$. Denotemos por $S$ al conjunto de los enteros $1, 2, \cdots, n$, esto es, el conjunto de enteros $i$ que satisfacen $1 \leqq i \leqq n$. Separemos a $S$ en los subconjuntos $S_d$, donde $d|n$, poniendo a $i$ en $S_d$ si $(i, n) = d$. Entonces cada elemento de $S$ está exactamente en un $S_d$. Además, $i$ está en $S_d$ si y solamente si es de la forma $jd$ con $1 \leqq j \leqq n/d$ y $(j, n/d) = 1$. Por lo tanto, existen exactamente $\phi(n/d)$ elementos en $S_d$. Supuesto que hay $n$ elementos en $S$, se tiene $n = \sum_{d|n} \phi(n/d)$ lo cual puede escribirse como $n = \sum_{d|n} \phi(d)$. Esto es el contenido del Teorema 2.17. Entonces, por el Teorema 4.7,

$$\phi(n) = \sum_{d|n} \mu(d) \frac{n}{d}, \qquad \frac{\phi(n)}{n} = \sum_{d|n} \frac{\mu(d)}{d}.$$

También la función $\mu(d)/d$ y, por el Teorema 4.4, también lo es $\phi(n)/n$. De aquí $\phi(n)$ es multiplicativa y se tiene el Teorema 2.15. Finalmente, usando la ecuación, anterior, remplazando $n$ por $p^e$, se tiene

$$\phi(p^e) = \sum_{d|p^e} \mu(d) \frac{p^e}{d} = \sum_{f=0}^{e} \mu(p^f) \frac{p^e}{p^f}$$

$$= \mu(1)p^e + \mu(p)p^{e-1} = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right)$$

si $e \geqq 1$, y de aquí que

$$\phi(p_1^{e_1}p_2^{e_2} \cdots p_r^{e_r}) = p_1^{e_1}p_2^{e_2} \cdots p_r^{e_r}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_r}\right)$$

dado que $\phi(n)$ es multiplicativa. Esto es el contenido del Teorema 2.16.

**Problemas**

1. Encontrar un entero positivo $n$ tal que $\mu(n) + \mu(n+1) + \mu(n+2) = 3$.
2. Probar que $\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$ si $n$ es un entero positivo.
3. Evaluar $\sum_{j=1}^{\infty} \mu(j!)$.
4. Probar el Teorema 4.8 definiendo $G(n)$ como $\sum_{d|n} f(d)$, entonces aplicando el Teorema 4.7 para escribir $f(n) = \sum_{d|n} \mu(d)G(n/d)$. De donde $\sum_{d|n} \mu(d)G(n/d) = \sum_{d|n} \mu(d)F(n/d)$. Usar esto para demostrar que $F(1) = G(1)$, $F(2) = G(2)$, $F(3) = G(3)$ y así sucesivamente.
5. Si $k$ denota el número de factores primos distintos de un entero positivo $n$, probar que $\sum_{d|n} |\mu(d)| = 2^k$.

6. Si $F(n) = \sum_{d|n} f(d)$ para todo entero positivo $n$, probar que $f(n) = \sum_{d|n} \mu(n/d)F(d)$.
7. Supóngase que $n$ tiene los factores primos distintos $p_1, p_2, \cdots, p_k$. Probar que $\sum_{d|n} \mu(d)\tau(d) = (-1)^k$. De modo semejante, evaluar $\sum_{d|n} \mu(d)\sigma(d)$.
8. Si $n$ es cualquier entero par, probar que $\sum_{d|n} \mu(d)\phi(d) = 0$.
9. Mediante el uso de la identidad algebraica $(x + 1)^2 - x^2 = 2x + 1$, establecer que $(n + 1)^2 - 1^2 = \sum_{x=1}^{n} \{(x + 1)^2 - x^2\} = \sum_{x=1}^{n} (2x + 1)$ y así llegar al resultado $\sum_{x=1}^{r} x = n(n + 1)/2$.
10. Mediante el uso de la identidad algebraica $(x + 1)^3 - x^3 = 3x^2 + 3x + 1$, establecer que $(n + 1)^3 - 1^3 = \sum_{x=1}^{n} \{(x + 1)^3 - x^3\} = \sum_{x=1}^{n} (3x^2 + 3x + 1)$ y así llegar al resultado $\sum_{x=1}^{n} x^2 = n(n + 1)(2n + 1)/6$. (Los resultados de este problema y el anterior pueden establecerse por otros métodos, por ejemplo, inducción matemática).
11. Supóngase que $S(n)$ denota la suma de los cuadrados de los enteros positivos $\leqq n$ y primos para $n$. Probar que

$$\sum_{j=1}^{n} j^2 = \sum_{d|n} d^2 S\left(\frac{n}{d}\right) = \sum_{d|n} \frac{n^2}{d^2} S(d).$$

*Sugerencia:* separar los enteros $\leqq n$ en clases, de manera que todos los enteros $k$ tales que $(k, n) = d$ se encuentren en la misma clase.
12. Combinar los resultados de los problemas anteriores para obtener

$$\sum_{d|n} \frac{S(d)}{d^2} = \frac{1}{6}\left(2n + 3 + \frac{1}{n}\right).$$

Entonces aplicar la fórmula de inversión de Moebius para obtener

$$\frac{S(n)}{n^2} = \sum_{d|n} \frac{1}{6}\mu(d)\left(\frac{2n}{d} + 3 + \frac{d}{n}\right).$$

13. Probar que $f(n) = n\mu(n)$ es una función multiplicativa y que $\sum_{d|n} d\mu(d) = (-1)^k\phi(n)p_1p_2\cdots p_k/n$ donde $p_1, p_2, \cdots, p_k$ son los factores primos distintos de $n$.
14. Combinar los resultados de los dos problemas anteriores para obtener $S(n) = n^2\phi(n)/3 + (-1)^k\phi(n)p_1p_2\cdots p_k/6$ para $n > 1$, donde como antes $p_1p_2, \cdots, p_k$ son los factores primos de $n$. *Sugerencia:* usar la fórmula $\sum_{d|n} \mu(d)/d = \phi(n)/n$.
15. Dado cualquier entero positivo $k$, probar que existe un número infinito de enteros $n$ tales que

$$\mu(n + 1) = \mu(n + 2) = \mu(n + 3) = \cdots = \mu(n + k).$$

## 4.4 Funciones de recurrencia

Puede definirse un tipo particular de función numérica de la manera siguiente. Si $a$, $b$, $x_0$, $x_1$ son números arbitrarios, incluso tal vez complejos, hagamos $f(0) = x_0$, $f(1) = x_1$ y $f(n+1) = af(n) + bf(n-1)$ para $n \geqq 1$. Esto determina unívocamente a $f(n)$, dependiendo solamente de $a$, $b$, $x_0$, $x_1$. Por conveniencia se escribirá $x_n$ en lugar de $f(n)$ y se tendrá $x_{n+1} = ax_n + bx_{n-1}$. Tal relación recibe el nombre de fórmula de recurrencia o de repetición.

Para obtener una relación más simple se escribe esta última ecuación en la forma

$$x_{n+1} - kx_n = (a-k)(x_n - kx_{n-1}) + (b + ak - k^2)x_{n-1}.$$

Si $k_1$ y $k_2$ son las raíces de $k^2 - ak - b = 0$, entonces $k_1 + k_2 = a$ y se tiene

$$x_{n+1} - k_1x_n = k_2(x_n - k_1x_{n-1}),$$

$$x_{n+1} - k_2x_n = k_1(x_n - k_2x_{n-1}),$$

y de aquí que

$$x_{n+1} - k_1x_n = k_2^n(x_1 - k_1x_0),$$

$$x_{n+1} - k_2x_n = k_1^n(x_1 - k_2x_0).$$

Restando se encuentra $(k_2 - k_1)x_n = (x_1 - k_1x_0)k_2^n - (x_1 - k_2x_0)k_1^n$. Por lo tanto, si $k_2 \neq k_1$, se tiene

$$(4.1) \qquad x_n = \frac{(x_1 - k_1x_0)k_2^n - (x_1 - k_2x_0)k_1^n}{k_2 - k_1}, \qquad k_2 \neq k_1.$$

Así se tiene la fórmula para encontrar el valor de $x_n$ directamente en términos de $a$, $b$, $x_0$, $x_1$ sin tener que calcular los valores de $x_2, x_3, \ldots, x_{n-1}$. Sin embargo, esta fórmula no tiene significado si $k_2 = k_1$. En este caso podríamos tratar de mantener fijos $k_1$ y $n$ y hacer que $k_2$ tienda hacia $k_1$, esperando que esto sugerirá una solución que, a continuación, podemos verificar. Consideremos la ecuación anterior como si tuviera la forma

$$x_n = \frac{g(k_2)}{h(k_2)}$$

con $g(k_1) = h(k_1) = 0$ y apliquemos la regla de L'Hospital en la forma

$$\lim_{k_2\to k_1} \frac{g(k_2)}{h(k_2)} = \lim_{k_2\to k_1} \frac{g'(k_2)}{h'(k_2)}$$

si el límite del segundo miembro existe. Esto nos lleva a

$$\lim_{k_2\to k_1} x_n = \lim_{k_2\to k_1} \{n(x_1 - k_1x_0)k_2^{n-1} + x_0k_1^n\} = nx_1k_1^{n-1} - nx_0k_1^n + x_0k_1^n.$$

Ahora podemos hacer $y_n = nx_1k_1^{n-1} - nx_0k_1^n + x_0k_1^n$ y comprobar realmente si $y_n$ es o no la solución. Dado que $k_1 = k_2$ es la única raíz de $k^2 - ak - b = 0$ se tiene $a = 2k_1$, $b = -k_1^2$. Se tiene $y_0 = x_0$, $y_1 = x_1$ y, para $n \geq 1$,

$$\begin{aligned} y_{n+1} &= (n+1)x_1k_1^n - (n+1)x_0k_1^{n+1} + x_0k_1^{n+1} \\ &= 2k_1(nx_1k_1^{n-1} - nx_0k_1^n + x_0k_1^n) \\ &\qquad - k_1^2\{(n-1)x_1k_1^{n-2} - (n-1)x_0k_1^{n-1} + x_0k_1^{n-1}\} \\ &= ay_n + by_{n-1}. \end{aligned}$$

Ahora bien, para $n \geqq 1$, se tiene $y_{n+1} - x_{n+1} = a(y_n - x_n) + b(y_{n-1} - x_{n-}$ y $y_0 - x_0 = 0$, $y_1 - x_1 = 0$. Esto implica que $y_{n+1} - x_{n+1} = 0$ para $n + 1 = 2, 3, 4, \ldots$ y se tiene

$$x_n = y_n = nx_1k_1^{n-1} - (n-1)x_0k_1^n, \qquad k_1 = k_2$$

En ambos casos, se han encontrado las fórmulas para $x_n$. Si $a$, $b$, $x_0$, $x_1$ son enteros, entonces también lo son todos los $x_n$, puesto que $x_n = ax_{n-1} + bx_{n-2}$.

Los números de Fibonacci $F_0, F_1, \ldots$ se definen por $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$. En este caso se tiene $k^2 - k - 1 = 0$, $k_1 = (1 - \sqrt{5})/2$, $k_2 = (1 + \sqrt{5})/2$ y, por la (4.1),

$$F_n = \frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right\}.$$

Como otro ejemplo considérese la sucesión 0, 1, 3, 8, 21, . . . , para la cual $x_0 = 0$, $x_1 = 1$, $a = 3$, $b = -1$. Entonces $k_1 = (3 - \sqrt{5})/2$, $k_2 = (3 + \sqrt{5})/2$ y

$$x_n = \frac{1}{\sqrt{5}}\left\{\left(\frac{3+\sqrt{5}}{2}\right)^n - \left(\frac{3-\sqrt{5}}{2}\right)^n\right\}.$$

Pero $0 < \{(3 - \sqrt{5})/2\}^n \leqq 1$ y $x_n$ es un entero de modo que, en este caso, puede escribirse la solución como

$$x_n = \left[\frac{1}{\sqrt{5}}\left(\frac{3+\sqrt{5}}{2}\right)^n\right].$$

**Problemas**

1. Sin usar los resultados de esta sección encontrar una fórmula para $x_n$ si $x_{n+1} = ax_n$. También si $x_{n+1} = bx_{n-1}$.
2. Encontrar una fórmula para $x_n$ si $x_{n+1} = 2x_n - x_{n-1}$, $x_0 = 0$, $x_1 = 1$. También si $x_0 = 1$, $x_1 = 1$. Entonces hacer lo mismo para $x_{n+1} = 2x_n + 3x_{n-1}$.
3. Escribir los primeros diez términos de la serie de Fibonacci. Probar que, en general, dos términos consecutivos cualesquiera son relativamente primos.

4. Probar que los números de Fibonacci satisfacen las desigualdades

$$\left(\frac{1+\sqrt{5}}{2}\right)^{n-1} < F_{n+1} < \left(\frac{1+\sqrt{5}}{2}\right)^{n},$$

si $n > 1$. *Sugerencia*: escribir $\alpha$ por $(1 + \sqrt{5})/2$ y observar que $\alpha^2 = \alpha + 1 > F_2 + F_1 = F_3$, $\alpha^3 = \alpha^2 + \alpha > F_3 + F_2 = F_4$. Entonces aplicar la inducción.

5. Probar que para $n \geqq 2$,

$$F_n = \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \binom{n-4}{3} + \cdots + \binom{n-j}{j-1},$$

donde la suma de los coeficientes binominales de la derecha termina con el mayor $j$ tal que $2j \leqq n + 1$. *Sugerencia*: aplicar el hecho de que $\binom{m}{r} = \binom{m-1}{r-1} + \binom{m-1}{r}$.

6. Probar que $F_1 + F_2 + F_3 + \cdots + F_n = F_{n+2} - 1$.
7. Probar que $F_{n-1}F_{n+1} - F_n^2 = (-1)^n$.
8. Probar que $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$ para cualesquiera enteros positivos $m$ y $n$. Entonces probar que $F_m | F_n$ si $m | n$. *Sugerencia*: hacer $n = mq$ y aplicar la inducción sobre $q$.
9. Considérese la sucesión $1, 2, 3, 5, 8, \cdots = F_2, F_3, F_4, F_5, F_6, \cdots$. Probar que todo entero positivo puede escribirse como una suma de términos de esta sucesión. *Sugerencia*: para un $k$ que no pertenece a la sucesión sea $n$ tal que $F_{n-1} < k < F_n$. Demostrar que $0 < k - F_{n-1} < F_{n-2}$. Probar la afirmación por inducción.
10. Denótese por $f(n)$ el número de sucesiones $a_1, a_2, \cdots, a_n$ que puedan construirse, donde cada $a_j$ es $+1$, $-1$ o bien $0$, sujeto a las restricciones de que dos términos consecutivos no pueden ser $+1$, ni dos términos consecutivos pueden ser $-1$. Probar que $f(n)$ es el entero más próximo a $\frac{1}{2}(1 + \sqrt{2})^{n+1}$. *Sugerencia*: probar que $f(n) = 2f(n-1) + f(n-2)$.
11. *a*) Sea $S_n$ un conjunto de enteros $x$, $1 \leqq x \leqq n$, tales que ningún miembro de $S_n$ divide a otro miembro de $S_n$. Demostrar que $S_n$ puede tener $[(n + 1)/2]$ miembros, pero no más.
*b*) Encontrar el número máximo de miembros de $S_n$ si los $x$ también se restringen a ser impares.
*c*) Demostrar que si $2^k a$, $a$ impar, está en el $S_n$ de (*a*) y si $S_n$ tiene el número máximo de miembros, entonces $n < 3^{k+1}a$.
*d*) Demostrar que un $S_n$ de (*a*) puede tener menos que el número máximo de miembros y, sin embargo, tener el máximo en el sentido de que ningún miembro nuevo puede adjuntarse a $S_n$.
12. Sea $f(n)$ la suma de los primeros $n$ términos de la sucesión $0, 1, 1, 2, 2, 3, 3, 4, 4, \cdots$. Construir una tabla para $f(n)$. Probar que $f(n) = [n^2/4]$. Para $x$, $y$, enteros, $x > y$, probar que $xy = f(x + y) - f(x - y)$. Por tanto el proceso de la multiplicación puede reemplazarse por una adición, una sustracción, seleccionando dos números de la tabla y sustrayéndolos.
13. Aplicar las ideas de esta sección para encontrar una fórmula para $x_n$ si $x_0 = 1$, $x_1 = 2$, $x_2 = 1$ y $x_{n+1} = x_n + 4x_{n-1} - 4x_{n-2}$. *Sugerencia*: considérese la expresión $x_{n+1} + kx_n + lx_{n-1}$.

# Capítulo 5

# Algunas ecuaciones diofantinas

## 5.1 Ecuaciones diofantinas

Existen muchos problemas y acertijos cuyas soluciones no requieren más que encontrar todas las soluciones de alguna ecuación. Se redactan en tal forma que las soluciones deseadas deben satisfacer otras condiciones. Por ejemplo, se observa que $\frac{26}{65} = \frac{2\not{6}}{\not{6}5} = \frac{2}{5}$ es correcta aunque esta cancelación de los 6 viola las reglas del álgebra. Nuestro problema es encontrar todas las fracciones positivas que se comportan en esta forma. Esto es, se desea determinar $x, y, z$ en tal forma que $\frac{10x + y}{10y + z} = \frac{x}{z}$. Esta expresión se reduce a $(y - x)z = 10(y - z)x$ pero solamente estamos interesados en las soluciones tales que $x$, $y$ y $z$ sean enteros positivos menores que 10. No llevaremos a cabo la resolución. No es difícil ver que las soluciones son $\frac{19}{95}, \frac{16}{64}, \frac{26}{65}, \frac{49}{98}$ y las fracciones de la forma $\frac{10x + x}{10x + x}$.

En el problema anterior, la ecuación $(y - x)z = 10(y - z)x$ es una ecuación indeterminada. Tiene muchas soluciones algebraicas y se requiere escoger las soluciones en las cuales $x$, $y$ y $z$ son enteros positivos menores que 10. Tal problema recibe el nombre de problema diofantino y se dice que se resuelve una ecuación diofantina. Este problema particular es simplemente una curiosidad pero existen muchas ecuaciones diofantinas importantes. En general, las restricciones que se agregan son que las soluciones deben ser enteros o, en ocasiones, racionales. Frecuentemente, las soluciones también deben ser positivas.

Existen variedades sin fin de las ecuaciones diofantinas y no se tiene un método general de solución. Se discutirán algunas de las ecuaciones más sencillas. También se considerarán algunos problemas relacionados. Por ejemplo, el Teorema 5.6 establece, en efecto, que la ecuación $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ tiene por lo menos una solución, $x_1$, $x_2$, $x_3$, $x_4$ enteros, para cada entero positivo $n$. Sin embargo, no intentaremos encontrar todas las soluciones enteras.

La ecuación de Pell, $x^2 - dy^2 = N$, se discutirá en el capítulo 7.

## 5.2 La ecuación $ax + by = c$

Cualquier ecuación lineal en dos variables que tenga coeficientes enteros puede ponerse en la forma $ax + by = c$. El problema es trivial, a menos que tanto $a$ como $b$ no sean cero, por tanto, supongamos que $a \neq 0$, $b \neq 0$. Denotemos $(a, b)$ por $g$. Entonces el Teorema 1.3 demuestra que existen los enteros $x_0$ y $y_0$ tales que $ax_0 + by_0 = g$. Los valores numéricos para $x_0$ y $y_0$ pueden obtenerse convenientemente aplicando el algoritmo euclidiano, Teorema 1.11, a los enteros $|a|$ y $|b|$.

Ahora bien, si $g \nmid c$, entonces $ax + by = c$ evidentemente no tiene solución en los enteros. Si $g|c$, se usa la solución $x_0$, $y_0$ de $ax + by = g$ para obtener una solución $x_1 = (c/g)x_0$, $y_1 = (c/g)y_0$ de $ax + by = c$. Con el objeto de encontrar todas las soluciones enteras, denotemos por $r, s$ cualquier solución entera. Entonces se tiene $ar + bs = c = ax_1 + by_1$ y de aquí que

$$(5.1) \qquad \frac{a}{g}(r - x_1) = -\frac{b}{g}(s - y_1).$$

Pero, por el Corolario 1.7, $(a/g, b/g) = 1$ y de aquí que $(a/g)|(s - y_1)$ y, por el Teorema 1.9, $(b/g)|(r - x_1)$. Esto implica $s - y_1 = (a/g)u$ y $r - x_1 = (b/g)t$ para algunos enteros $u$, $t$ y, entonces, (5.1) implica $u = -t$. Por lo tanto, toda solución entera $r, s$ de $ax + by = c$ puede escribirse en la forma $r = x_1 + (b/g)t$, $s = y_1 - (a/g)t$. Dado que estos valores evidentemente satisfacen $ax + by = c$, se ha resuelto la ecuación diofantina. Obsérvese que la ecuación tiene soluciones si y solamente si $(a, b)$ divide a $c$.

**Problemas**

1. Probar que todas las soluciones de $3x + 5y = 1$ pueden escribirse en la forma $x = 2 + 5t$, $y = -1 - 3t$; también en la forma $x = 2 - 5t$, $y = -1 + 3t$; también en la forma $x = -3 + 5t$, $y = 2 - 3t$. Probar que $x = a + bt$, $y = c + dt$ es una forma de la solución general si y solamente si $a$, $c$ es una solución y ya sea $b = 5$, $d = -3$ o bien $b = -5$, $d = 3$.
2. Encontrar todas las soluciones de $10x - 7y = 17$.

3. Si $ax + by = c$ es resoluble, probar que tiene una solución $x_0$, $y_0$ con $0 \leqq x_0 < |b|$.
4. Probar que $ax + by = a + c$ es resoluble si y solamente si $ax + by = c$ es resoluble.
5. Considérese la ecuación $ax + by = c$. Dado que puede dividirse entre cualquier factor común de los coeficientes, puede suponerse que $(a, b, c) = 1$. Probar que la ecuación es resoluble si y solamente si $(a, b) = 1$. Entonces suponiendo que $(a, b) = 1$, probar que la solución general es $x = x_1 + bt$, $y = y_1 - at$ donde $x_1$, $y_1$ es cualquier solución particular.
6. Probar que $ax + by = c$ es resoluble si y solamente si $(a, b) = (a, b, c)$.
7. Dado que $ax + by = c$ tiene dos soluciones $(x_0, y_0)$ y $(x_1, y_1)$ con $x_1 = 1 + x_0$ y dado que $(a, b) = 1$, probar que $b = \pm 1$.
8. Interpretadas geométricamente, las soluciones de $ax + by = c$ en los enteros son ciertos puntos sobre la línea recta representada por la ecuación en un sistema coordenado $x$, $y$. Si $(a, b) = 1$, probar que cualquier segmento de la línea de longitud $(a^2 + b^2)^{1/2}$ contiene por lo menos uno de estos puntos con coordenadas enteras.
9. Encontrar las condiciones necesarias y suficientes para que

$$x + b_1 y + c_1 z = d_1, \qquad x + b_2 y + c_2 z = d_2$$

tengan por lo menos una solución simultánea en los enteros $x$, $y$, $z$, suponiendo que los coeficientes son enteros con $b_1 \neq b_2$.
10. Dar una demostración independiente de que $ax + by = c$ tiene por lo menos una solución en los enteros $x$, $y$ si $(a, b)/c$ aplicando la inducción sobre máx $(a, b)$. *Sugerencia*: Si $0 < a < b$ entonces $ax + by = c$ es resoluble si y solamente si $a(x - y) + (b - a)y = c$ es resoluble.

## 5.3 Soluciones positivas

Supongamos que $a$, $b$ y $c$ son positivos, que $(a, b)|c$ y se desea encontrar todas las soluciones $r$, $s$ de $ax + by = c$ en enteros positivos. Se resuelve como en la Sección 5.2 y únicamente debe restringirse $t$ de tal manera que $r$ y $s$ sean positivos. Simplemente se restringe $t$ al rango $-(g/b)x_1 < t < (g/a)y_1$. El menor valor permisible para $t$ es $[-(g/b)x_1 + 1]$ y el valor mayor es $-[(-g/a)y_1 + 1]$. Entonces, el número de soluciones es

$$\begin{aligned} N &= -\left[-\frac{g}{a}y_1 + 1\right] - \left[-\frac{g}{b}x_1 + 1\right] + 1 \\ &= -\left(\left[-\frac{g}{a}y_1\right] + \left[-\frac{g}{b}x_1\right] + 1\right) \end{aligned}$$

a partir de lo cual, aplicando el Teorema 4.1$d$, se encuentra que

$$-\left(\left[-\frac{g}{a}y_1 - \frac{g}{b}x_1\right] + 1\right) \leqq N \leqq -\left[-\frac{g}{a}y_1 - \frac{g}{b}x_1\right].$$

Supuesto que $-(g/a)y_1 - (g/b)x_1 = -(g/ab)(by_1 + ax_1) = -(gc)/(ab)$, finalmente se tiene

$$-\left[-\frac{gc}{ab}\right] - 1 \leqq N \leqq -\left[-\frac{gc}{ab}\right].$$

Estas desigualdades no constituyen una fórmula precisa para $N$, pero especifican dos enteros consecutivos uno de los cuales debe ser $N$. Obsérvese que siempre existirá por lo menos una solución positiva de $ax + by = c$ si $g|c$ y $gc > ab$.

**Problemas**

1. Encontrar todas las soluciones en enteros positivos:
   (*a*) $5x + 3y = 52$;
   (*b*) $15x + 7y = 111$;
   (*c*) $40x + 63y = 521$;
   (*d*) $123x + 57y = 531$;
   (*e*) $12x + 501y = 1$;
   (*f*) $12x + 501y = 274$;
   (*g*) $97x + 98y = 1000$.
2. Probar que $101x + 37y = 3819$ tiene una solución positiva en enteros.
3. Dado que $(a, b) = 1$ y que $a$ y $b$ son de signos opuestos, probar que $ax + by = c$ tiene un número infinito de soluciones positivas para cualquier valor de $c$.
4. Sean los enteros positivos $a, b, c$. Probar que no existe solución de $ax + by = c$ en los enteros positivos si $a + b > c$.
5. La teoría del texto establece que una de las fórmulas
$$N = -\left[-\frac{gc}{ab}\right] - 1, \qquad N = -\left[-\frac{gc}{ab}\right]$$
es correcta. Probar que ninguna de las fórmulas es correcta en todos los casos.
6. Sean los enteros positivos $a, b, c$ tales que $(a, b) = 1$. Suponiendo que $c/ab$ no es un entero, probar que el número $N$ de soluciones de $ax + by = c$ en enteros positivos es $[c/ab]$ o bien $[c/ab] + 1$. Suponiendo además que $c/a$ es un entero, probar que $N = [c/ab]$. *Sugerencia:* si $c/a$ es un entero, entonces puede encontrarse fácilmente una solución específica de $ax + by = c$, por ejemplo, $x_1 = c/a$, $y_1 = 0$.
7. Sean $a, b, c$ enteros positivos tales que $(a, b) = 1$. Suponiendo que $c/ab$, es un entero, probar que $N = -1 + c/ab$.
8. Modificar la teoría de esta sección de modo que trate al número, digamos $N_0$, de soluciones en enteros no negativos de $ax + by = c$, donde $a, b, c$ son enteros positivos tales que $(a, b)|c$. *Sugerencia:* obsérvese que $t$ se restringe al rango $-(g/b)x_1 \leqq t \leqq (g/a)y_1$. El menor valor permisible para $t$ es $-[(g/b)x_1]$ y el valor mayor es $[(g/a)y_1]$. Las desigualdades finales resultan
$$\left[\frac{gc}{ab}\right] \leqq N_0 \leqq \left[\frac{gc}{ab}\right] + 1.$$
9. Sean $a$ y $b$ enteros positivos que satisfacen $(a, b) = 1$. Considérese el conjunto $S$ de enteros $\{ax + by\}$, donde $x$ y $y$ recorren todos los enteros

no negativos. Probar que el conjunto $S$ contiene todos los enteros mayores que $c = ab - a - b$, pero no el propio $c$.

10. En el problema anterior, restringir $x$ y $y$ a que sean enteros positivos, obteniendo el conjunto $S' = \{ax + by\}$ ¿Cuál es el entero mayor no contenido en el conjunto $S'$?

## 5.4 Otras ecuaciones lineales

Considérese la ecuación

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = c, \qquad k > 2, \tag{5.2}$$

y denótese por $g$ el máximo común divisor $(a_1, a_2, \ldots, a_k)$. Si la ecuación tiene una solución, entonces evidentemente $g|c$. Inversamente, por el Teorema 1.5, existe $y_1, y_2, \ldots, y_k$ tal que $a_1y_1 + a_2y_2 + \cdots, + a_ky_k = g$. Si $g|c$ entonces $c = gr$ para algún entero $r$ y $x_1 = ry_1$, $x_2 = ry_2, \ldots, x_k = ry_k$ es una solución de (5.2). Por tanto, (5.2) tiene soluciones si y solamente si $g|c$.

Para encontrar las soluciones de (5.2) se reduce al caso de la Sección 5.2 con dos incógnitas. Puede suponerse que los $a_i$ no son cero y que $(a_1, a_2, \ldots, a_k)|$c. Se escribe

$$x_{k-1} = \alpha u + \beta v, \qquad x_k = \gamma u + \delta v, \tag{5.3}$$

donde se escogerán los enteros $\alpha$, $\beta$, $\gamma$, $\delta$ en tal forma que $\alpha\delta - \beta\gamma = 1$. Entonces se tendrá $u = \delta x_{k-1} - \beta x_k$ y $v = -\gamma x_{k-1} + \alpha x_k$. Así que, $u$ y $v$ son enteros si y solamente si $x_{k-1}$, $x_k$ lo son. Si se toma

$$\beta = \frac{a_k}{(a_{k-1}, a_k)} \qquad \delta = \frac{-a_{k-1}}{(a_{k-1}, a_k)},$$

entonces $(\beta, \delta) = 1$ y puede resolverse $\alpha\delta - \beta\gamma = 1$ para $\alpha$, $\gamma$ por el método de la Sección 5.2. Sin embargo, sólo se necesita un par de valores para $\alpha$, $\gamma$, no la solución general.

Ahora la ecuación (5.2) se reduce a

$$a_1x_1 + a_2x_2 + \cdots + a_{k-2}x_{k-2} + (a_{k-1}\alpha + a_k\gamma)u = c, \tag{5.4}$$

con una incógnita menos y se observa que

$$a_{k-1}\alpha + a_k\gamma = -(a_{k-1}, a_k)\alpha\delta + (a_{k-1}, a_k)\beta\gamma = -(a_{k-1}, a_k),$$
$$(a_1, a_2, \ldots, a_{k-2}, (a_{k-1}, a_k)) = (a_1, a_2, \ldots, a_k).$$

De donde, la nueva ecuación, (5.4), tiene las mismas propiedades que la ecuación (5.2), que el m. c. d. de sus coeficientes divide a $c$ y que ningún coeficiente es cero. Si $k > 3$ puede aplicarse este proceso de reducción a la ecuación (5.4) para producir una ecuación con $k - 2$ variables y, por tanto, las repeticiones del proceso conducen finalmente a una ecuación con dos incógnitas.

Además puede observarse, de la Sección 5.2, que si una ecuación lineal en dos incógnitas tiene una solución, su solución general está dada en términos de un solo parámetro $t$. De modo semejante, las soluciones de (5.2), con $k$ incógnitas, se expresan en términos de $k - 1$ parámetros. Esto puede probarse por inducción sobre $k$. Porque si cualquier ecuación tal como (5.4), en $k - 1$ incógnitas, tiene las soluciones $x_1, x_2, \cdots, x_{k-2}, u$ en términos de $k - 2$ parámetros $v_1, v_2, \cdots, v_{k-2}$, entonces, por (5.3), las soluciones de (5.2) están dadas por $x_1, x_2, \cdots, x_{k-2}, \alpha u + \beta v, \gamma u + \delta v$. Estas contienen los $k - 1$ parámetros $v_1, v_2, \cdots, v_{k-2}, v$. Es fácil ver que las soluciones tienen la forma $x_i = b_i + d_{i,1}v_1 + d_{i,2}v_2 + \cdots + d_{i,k-1}v_{k-1}$ donde se ha escrito $v_{k-1}$ por $v$.

Si se pidiera resolver un sistema de $s$ ecuaciones en $r$ incógnitas,

$$(5.5) \qquad a_{j,1}x_1 + a_{j,2}x_2 + \cdots + a_{j,r}x_r = c_j, \qquad j = 1, 2, \cdots, s,$$

se empieza por resolver la primera ecuación, $j = 1$. Si tiene una solución, será de la forma

$$x_i = b_i + d_{i,1}v_1 + d_{i,2}v_2 + \cdots + d_{i,r-1}v_{r-1}, \qquad i = 1, 2, \cdots, r.$$

Se sustituyen éstas en las ecuaciones restantes y se vuelve la segunda ecuación, $j = 2$, para $v_1, v_2, \cdots, v_{r-1}$ en términos de $r - 2$ nuevos parámetros. La repetición de este proceso nos permite resolver el sistema (5.5). Por supuesto que, si se encuentra una ecuación que no tiene soluciones, entonces el sistema (5.5) no tiene soluciones.

**Problema**

1. Resolver las ecuaciones:

(*a*) $x + 2y + 3z = 1$ (*d*) $5x - 2y - 4z = 10$
(*b*) $x + 2y + 3z = 10$ (*e*) $3x - 6y + 5z = 11$
(*c*) $5x - 2y - 4z = 1$ (*f*) $6x + 48y - 78z = 5$

## 5.5 La ecuación $x^2 + y^2 = z^2$

Se desea resolver la ecuación $x^2 + y^2 = z^2$ en enteros positivos. Considérese una solución de ese tipo $x, y, z$ y escribir $g$ por $(x, y)$. Entonces $g^2 \mid z^2$ y de aquí que $g \mid z$ y puesto que, en general, $(x, y, z) = ((x, y), z)$ se cumple, se ve que $(x, y, z) = g$. Por simetría se tiene $(x, y, z) = (x, y) = (y, z) = (x, z) = g$, y

$$\left(\frac{x}{g}\right)^2 + \left(\frac{y}{g}\right)^2 = \left(\frac{z}{g}\right)^2, \qquad \left(\frac{x}{g}, \frac{y}{g}\right) = \left(\frac{y}{g}, \frac{z}{g}\right) = \left(\frac{x}{g}, \frac{z}{g}\right) = 1.$$

Una solución $x_1, y_1, z_1$ que tiene la propiedad de que estos tres son relativamente primos en pares recibe el nombre de solución primitiva. Por

tanto, toda solución $x, y, z$ puede escribirse en la forma $gx_1, gy_1, gz_1$, donde $x_1, y_1, z_1$ es alguna solución primitiva. Inversamente, si $x_1, y_1, z_1$ es una solución primitiva, entonces $gx_1, gy_1, gz_1$ es una solución si $g$ es un entero positivo. Por tanto, sólo es necesario obtener las soluciones primitivas y así se hará a continuación.

Ahora bien, $x$ y $y$ no pueden ser ambos pares. Tampoco pueden ser ambos impares porque si lo fueran se tendría $x^2 \equiv 1 \pmod 4$, $y^2 \equiv 1 \pmod 4$ y, por lo tanto, $z^2 \equiv 2 \pmod 4$, lo cual es imposible.

Dado que $x$ y $y$ entran en las ecuaciones simétricamente ahora podemos restringir nuestra atención a las soluciones primitivas para las cuales $y$ es par, $x$ y $z$ impares. Entonces se tiene

$$\frac{z+x}{2}\frac{z-x}{2} = \left(\frac{y}{2}\right)^2. \tag{5.6}$$

Ahora
$$\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \Big| \left(\frac{z+x}{2} + \frac{z-x}{2}\right) = z$$

y
$$\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \Big| \left(\frac{z+x}{2} - \frac{z-x}{2}\right) = x$$

y por tanto
$$\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1.$$

Esto, con la ecuación (5.6), demuestra que $(z + x)/2 = r^2$ y $(z - x)/2 = s^2$ para algunos enteros positivos $r, s$. También se ve que $(r, s) = 1$, $r > s, x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$. También, supuesto que $z$ es impar, $r$ y $s$ son de paridad opuesta, uno es par, el otro impar.

Inversamente, sean $r$ y $s$ dos enteros cualesquiera tales que $(r, s) = 1$, $r > s > 0$, $r$ y $s$ de paridad opuesta. Entonces, si $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$, se tienen $x, y, z$ positivos y

$$x^2 + y^2 = (r^2 - s^2)^2 + (2rs)^2 = (r^2 + s^2)^2 = z^2.$$

Es fácil ver que $(x, y) = 1$ y que $y$ es par. Por tanto, $x, y, z$ es una solución primitiva con $y$ par. Así se tiene el siguiente resultado.

**Teorema 5.1** *Las soluciones primitivas positivas de $x^2 + y^2 = z^2$ con $y$ par son $x = r^2 - s^2$, $y = 2rs$, $z = r^2 + s^2$, donde $r$ y $s$ son enteros arbiratrios de paridad opuesta con $r > s > 0$ y $(r,s) = 1$.*

**Problemas**

1. Encontrar todas las soluciones primitivas de $x^2 + y^2 = z^2$, teniendo $0 < z < 30$.
2. Probar que si $x^2 + y^2 = z^2$, entonces uno de $x, y$ es un múltiplo de 3 y uno de $x, y, z$ es un múltiplo de 5.

3. Cualquier solución de $x^2 + y^2 = z^2$ en enteros positivos recibe el nombre de tripleta pitagoreana debido a que existe un triángulo rectángulo cuyos lados tienen las correspondientes longitudes. Encontrar todas las tripletas pitagoreanas cuyos términos forman $(a)$ una progresión aritmética, $(b)$ una progresión geométrica.
4. Si $n$ es cualquier entero $\geqq 3$, demostrar que existe una tripleta pitagoreana con $n$ como uno de sus miembros.
5. ¿Para cuales enteros positivos $n$ existen soluciones para la ecuación $x^2 - y^2 = n$?
6. Probar que todo entero $n$ puede expresarse en la forma $n = x^2 + y^2 - z^2$.
7. Probar que $x^2 + y^2 = z^4$ tiene un número infinito de soluciones con $(x, y, z) = 1$.
8. Demostrar que todas las soluciones de $x^2 + 2y^2 = z^2$ en enteros positivos con $(x, y, z) = 1$ están dadas por $x = |u^2 - 2v^2|$, $y = 2uv$, $z = u^2 + 2v^2$, donde $u$ y $v$ son enteros positivos arbitrarios tales que $u$ es impar y $(u, v) = 1$. *Sugerencia*: cualquier solución tiene $y$ par, puesto que $y$ impar implica $z^2 - x^2 \equiv 2 \pmod 8$, lo cual es imposible. De aquí que $x$ y $z$ son impares y puede usarse como modelo la demostración del Teorema 5.1.
9. Demostrar que $(x, y) > 1$ si $x, y, z$ satisface $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$.
10. Demostrar que si $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$, entonces $xy \equiv 0 \pmod{60}$.
11. Probar que las soluciones positivas de $\frac{1}{x^2} + \frac{1}{y^2} = \frac{1}{z^2}$, $(x, y, z) = 1$ están dadas por

$$x = r^4 - s^4, \quad y = 2rs(r^2 + s^2), \quad z = rs(r^2 - s^2)$$

o bien

$$x = 2rs(r^2 + s^2), \quad y = r^4 - s^4, \quad z = rs(r^2 - s^2)$$

donde $r > s > 0$, $(r, s) = 1$ y $r$ y $s$ de paridad opuesta.
12. Probar que ninguna tripleta pitagoreana de enteros pertenece a un triángulo rectángulo isósceles pero que existe un número infinito de tripletas pitagoreanas primitivas para las cuales los ángulos agudos de los triángulos correspondientes son, para cualquier positivo dado $\epsilon$, a $\epsilon$ de $\pi/4$.

## 5.6 La ecuación $x^4 + y^4 = z^2$

Al tratar de resolver la ecuación $x^4 + y^4 = z^2$ en enteros positivos, podemos restringirnos a las soluciones $x, y, z$ para las cuales $(x, y) = 1$, precisamente como en la Sección 5.5. Entonces $(x^2)^2 + (y^2)^2 = z^2$ y $x^2, y^2, z$ es una solución primitiva de la ecuación de la Sección 5.5. Puede suponerse que $y^2$, y por tanto $y$, es par. Entonces existen dos enteros $u$ y $v$ tales que $x^2 = u^2 - v^2$, $y^2 = 2uv$, $z = u^2 + v^2$, $u > v > 0$, $(u, v) = 1$ y $u$ y $v$ son de paridad opuesta. Si $u$ fuera par, entonces $v$ sería impar y se tendría $x^2 \equiv 0 - 1 \equiv 3 \pmod 4$. Dado que esto es imposible se tiene $u$ impar y $v$ par. Entonces

$$\left(\frac{y}{2}\right)^2 = u \cdot \frac{v}{2}, \qquad \left(u, \frac{v}{2}\right) = 1,$$

y de aquí que, para algunos enteros $r$ y $s$,

$$u = r^2, \frac{v}{2} = s^2, \quad y = 2rs, \quad (r, s) = 1, \quad r > 0, s > 0, \quad r \text{ impar.}$$

También $x^2 + v^2 = u^2$ de modo que se tiene $x^2 + 4s^4 = r^4$. Supuesto que $(r, 2s) = 1$, puede aplicarse la Sección 5.5 a esta ecuación. Existen los enteros $\rho$ y $\sigma$ tales que

$$x = \rho^2 - \sigma^2,\ 2s^2 = 2\rho\sigma,\ r^2 = \rho^2 + \sigma^2,\ (\rho, \sigma) = 1,\ \rho > \sigma > 0.$$

Ya que $\rho\sigma = s^2$, puede escribirse $\rho = f^2$, $\sigma = g^2$ con algunos $f > 0$, $g > 0$, $(f, g) = 1$. Entonces se tiene $r^2 = f^4 + g^4$, la cual se mira precisamente como la ecuación original. Al tratar de resolver la ecuación se ha tratado de reducirla a algo más sencillo pero se ha finalizado con una ecuación de la misma forma. A primera vista, esto parece más bien inútil, pero es posible que se haya ganado algo. Empezamos con la solución $x, y, z$ y finalizamos con la solución $f, g, r$. Es posible que se haya encontrado una solución diferente. De hecho se tiene $z = u^2 + v^2 = r^4 + 4s^4 > r^4$, de modo que $z > r$ y $f, g, r$ es una solución diferente. Más que esto, se ha obtenido una solución con $z > r > 0$. Ahora, si aplicamos la reducción completa a la nueva solución se obtiene todavía otra solución $f_1, g_1, r_1$, con $r > r_1 > 0$. Continuando en la misma forma se obtiene una sucesión completa de soluciones con correspondientes $r_i$ tales que $r > r_1 > r_2 > \cdots > 0$. Pero todos los $r_i$ son enteros y de aquí que $r_r \leqq 0$. Por lo tanto, la suposición de que hubiera una solución ha conducido a una contradicción. No se ha resuelto la ecuación pero se ha demostrado que no tiene solución $x, y, z$ en enteros positivos con $(x, y) = 1$.

Si $x, y, z$ fuera cualquier solución entera de la ecuación con $xy \neq 0$, entonces $|x|/g$, $|y|/g$, $|z|/g^2$ donde $g = (x, y)$ sería una solución en enteros positivos con $(|x|/g, |y|/g) = 1$.

Por lo tanto, cualquier solución $x, y, z$ será tal que $xy = 0$ y así se ha probado la siguiente proposición.

**Teorema 5.2** *Las únicas soluciones enteras de $x^4 + y^4 = z^2$ son las soluciones triviales $x = 0$, $y$, $z = \pm y^2$ y $x$, $y = 0$, $z = \pm x^2$.*

Al método usado en la demsotración de este Teorema en ocasiones se le da el nombre de "demostración por descenso" o bien "método del descenso infinito de Fermat". Este tipo de demostración, que también se presenta en otras ocasiones en la teoría de los números, se basa en el principio de que todo conjunto no vacío de enteros positivos contiene un elemento menor. También puede observarse que la demostración

podría haberse escrito en una forma ligeramente diferente como una reducción a una contradicción. Así, se ha supuesto que la solución inicial $x, y, z$ se ha seleccionado como ésa con el menor positivo $z$, el procedimiento nos hubiera conducido hacia otra solución $f, g, r$ con $0 < r < z$, lo cual evidentemente es una contradicción.

El hecho de que $x^4 + y^4 = z^2$ no tenga soluciones positivas implica que $x^4 + y^4 = z^4$ no tiene soluciones positivas. Este es un caso particular de una famosa proposición de Fermat. Con frecuencia se le nombra como el último teorema de Fermat y establece que para $n > 2$, las ecuaciones $x^n + y^n = z^n$ no tienen soluciones enteras diferentes a las soluciones triviales en las cuales una de las variables es cero. Se han encontrado las soluciones para $n = 2$ y se ha probado la proposición para $n = 4$. Se sabe que la proposición es verdadera para un gran número de valores de $n$, pero, en general, ni se ha probado ni se ha refutado.

**Problemas**

1. Para todo entero positivo $n \equiv 0 \pmod 4$, probar que $x^n + y^n = z^n$ no tiene soluciones con $xy \neq 0$.
2. Probar que $x^4 + 4y^4 = z^2$ no tiene soluciones con $xy \neq 0$. *Sugerencia*: usar el método de demostración del Teorema 5.2
3. Probar que $x^4 - y^4 = z^2$ no tiene soluciones con $yz \neq 0$.
4. Considérese un triángulo rectángulo entero, esto es, un triángulo rectángulo cuyas longitudes de los lados forman una tripleta pitagoreana. Probar que el área no es un cuadrado perfecto.
5. Probar que no hay enteros positivos $a$ y $b$ tales que tanto $a^2 + b^2$ como $a^2 - b^2$ son cuadrados perfectos.

## 5.7 Suma de cuatro cuadrados

Nuestra mira en esta sección no es resolver una ecuación diofantina sino solamente demostrar que la ecuación $x_1^2 + x_2^2 + x_3^2 + x_4^2 = n$ tiene por lo menos una solución entera siempre que $n$ sea un entero positivo. Empecemos con una identidad algebraica.

**Lema 5.3** *Se tiene*

$$(5.7)\quad (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2)$$
$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2$$
$$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.$$

*Demostración.* Esta identidad, descubierta por Euler, puede verificarse precisamente multiplicando ambos miembros.

Esta identidad muestra que si $X$ y $Y$ pueden expresarse como sumas de cuatro cuadrados, también puede expresarse su producto $XY$. Dado

que $1 = 1^2 + 0^2 + 0^2 + 0^2$ y $2 = 1^2 + 1^2 + 0^2 + 0^2$, sólo es necesario probar que todo primo impar puede expresarse como una suma de cuatro cuadrados. La demostración puede dividirse en dos pasos.

**Teorema 5.4** *Denotemos por $p$ cualquier primo impar. Existe un entero $m$ tal que $1 \leqq m < p$ y $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ para algunos enteros $x_1, x_2, x_3, x_4$.*

*Demostración.* Considérense los conjuntos $S_1$ consistente de $0^2, 1^2, 2^2, \cdots, \{(p-1)/2\}^2$ y $S_2$ consistente de $-0^2 - 1, -1^2 - 1, -2^2 - 1, \cdots, -\{(p-1)/2\}^2 - 1$. Dado que $x^2 \equiv y^2 \pmod p$ implica $p|(x-y)$ o bien $p|(x+y)$, se ve que no existen dos números de $S_1$ que sean congruentes módulo $p$. También no existen dos números de $S_2$ que sean congruentes módulo $p$. Ahora bien $S_1$ y $S_2$ juntos consisten de $p + 1$ enteros. Ya que existen solamente $p$ clases de residuos distintos módulo $p$ se ve que algún número, digamos $x^2$, es congruente módulo $p$ a algún número, $-y^2 - 1$, de $S_2$. Entonces $x^2 + y^2 + 1 \equiv 0 \pmod p$, $0 \leqq x \leqq (p-1)/2$, $0 \leqq y \leqq (p-1)/2$, y se tiene

$$x^2 + y^2 + 1 = mp, \qquad 1 \leqq m = \frac{1}{p}(x^2 + y^2 + 1)$$

$$\leqq \frac{1}{p}\left(2\left(\frac{p-1}{2}\right)^2 + 1\right) < \frac{1}{p}\left(\frac{p^2}{2} + 1\right) < p.$$

**Teorema 5.5** *Si $m$ es el menor entero que satisface el Teorema* 5.4, *entonces $m = 1$.*

*Demostración.* Evidentemente que existe por lo menos uno de esos $m$. Si $m$ es par, entonces también lo es $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$ y de aquí que ni uno, ni dos, ni cuatro de los $x_i$ son pares. Si exactamente dos de los $x_i$ son pares, podemos numerar los $x_i$ en tal forma que $x_1$ y $x_2$ son los pares. Entonces, en todos los casos $x_1 \pm x_2$ y $x_3 \pm x_4$ son pares, y

$$\left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2 = \frac{m}{2}p.$$

Por tanto, $m$ no es el menor si es par.

Ahora considérese la posibilidad $m > 1$. Supuesto que $m$ es impar se tiene $3 \leqq m < p$. Para $1 \leqq i \leqq 4$, se definen los números $y_i$ por

$$(5.8) \qquad y_i \equiv x_i \pmod m, \qquad -\frac{m-1}{2} \leqq y_i \leqq \frac{m-1}{2}.$$

Entonces $y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod m$ dado que $x_1^2 + x_2^2 + x_3^2 + x_4^2 = mp$ y puede escribirse

$$(5.9) \quad y_1^2 + y_2^2 + y_3^2 + y_4^2 = mn, \qquad 0 \leqq n \leqq \frac{1}{m}4\left(\frac{m-1}{2}\right)^2 < m.$$

Si $n$ fuera cero, por (5.9), se tendría $y_1 = y_2 = y_3 = y_4 = 0$ y entonces, por (5.8), $x_1 \equiv x_2 \equiv x_3 \equiv x_4 \equiv 0 \pmod{m}$. Esto implicaría que $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m^2}$, de aquí que $p \equiv 0 \pmod{m}$, lo cual es imposible supuesto que $3 \leqq m < p$. Por tanto, se tiene $n > 0$.

Aplicando el Teorema 5.3 se ve que

$$\text{(5.10)} \qquad \begin{aligned} m^2np &= (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= A_1^2 + A_2^2 + A_3^2 + A_4^2, \end{aligned}$$

donde los $A_i$ denotan las expresiones cuyos cuadrados aparecen en el segundo miembro de (5.7). Aplicando (5.8) fácilmente se encuentra que $A_i \equiv 0 \pmod{m}$ para $i = 1, 2, 3, 4$. Dividiendo (5.10) entre $m^2$ se obtiene

$$np = \left(\frac{A_1}{m}\right)^2 + \left(\frac{A_2}{m}\right)^2 + \left(\frac{A_3}{m}\right)^2 + \left(\frac{A_4}{m}\right)^2$$

con $0 < n < m$. Esto demuestra que $m$ no es el menor si $m > 1$. De aquí que $m = 1$ y el teorema queda demostrado.

Reuniendo los resultados y observando que $7 = 2^2 + 1^2 + 1^2 + 1^2$ requiere cuatro cuadrados, se obtiene el siguiente teorema:

**Teorema 5.6** *Todo entero positivo es una suma de cuatro cuadrados y menos de cuatro cuadrados no bastarán.*

**Problemas**

1. Probar que ningún entero de la forma $8k + 7$ puede expresarse como una suma de tres cuadrados.
2. Probar que ningún entero de la forma $4^m(8k + 7)$ es expresable como una suma de tres cuadrados. (*Observación:* éstos son los únicos enteros que no son expresables como sumas de tres cuadrados, pero la demostración de este resultado no se da en este libro).

## 5.8 Problema de Waring

Waring consideró la cuestión de cómo generalizar los resultados de la Sección 5.7 a potencias superiores.

Conjeturó que 9 cubos, 19 cuartas potencias, etc., bastarían. Hilbert probó que para cada entero positivo $k$ existe un número $g$ tal que las $g$-ésimas potencias bastarán. Si $g(k)$ denota el menor número de $k$-ésimas potencias que bastarán, entonces, tal y como ya se vio, $g(2) = 4$. Se sabe que $g(3) = 9$ y también se conoce el valor de $g(k)$ para $k \geqq 6$ aparte de una posible circunstancia excepcional relacionada a la parte fraccionaria de $(3/2)^k$. Para los casos $k = 4$ y 5 se sabe que $19 \leqq g(4) \leqq 35$ y $37 \leqq g(5) \leqq 54$. No obstante, excepto para $g(2)$ y $g(3)$, las demostraciones conocidas de estos resultados involucran métodos mucho

más complicados. Las demostraciones se apoyan principalmente en la teoría de las funciones de una variable compleja y pertenecen a la parte de la teoría de los números llamada teoría analítica de los números. Se tiene una buena parte de la historia del problema en las notas que se encuentran al final del capítulo 21 del libro *An Introduction to the Theory of Numbers* escrito por Hardy y Wright.

**Problema**

1. Probar que $g(k) \geqq 2^k + [3^k/2^k] - 2$. *Sugerencia:* expresar el número $n = 2^k[3^k/2^k] - 1$ como una suma de $k$-ésimas potencias.

## 5.9 Suma de cuartas potencias

Existe un pequeño resultado relacionado con el problema de Waring que puede obtenerse de modo muy sencillo. Se probará que $g(4) \leqq 50$. Esto está lejos del conocido resultado $g(4) \leqq 35$ pero tiene interés ya que la demostración es elemental y porque prueba la existencia de $g(4)$.

Sumando la identidad $(x_i + x_j)^4 + (x_i - x_j)^4 = 2x_i^4 + 12x_i^2x_j^2 + 2x_j^4$ se encuentra

$$\sum_{1 \leqq i < j \leqq 4} ((x_i + x_j)^4 + (x_i - x_j)^4)$$

$$= 2\sum_{i=1}^{4} (4 - i)x_i^4 + 6\sum_{i=1}^{4}\sum_{\substack{j=1 \\ j \neq i}}^{4} x_i^2x_j^2 + 2\sum_{j=1}^{4} (j - 1)x_j^4$$

$$= 2\sum_{i=1}^{4} (4 - i + i - 1)x_i^4 + 6\sum_{i=1}^{4}\sum_{\substack{j=1 \\ j \neq i}}^{4} x_i^2x_j^2$$

$$= 6\sum_{i=1}^{4} x_i^4 + 6\sum_{i=1}^{4}\sum_{\substack{j=1 \\ j \neq i}}^{4} x_i^2x_j^2$$

$$= 6\sum_{i=1}^{4}\sum_{j=1}^{4} x_i^2x_j^2 = 6\left(\sum_{i=1}^{4} x_i^2\right)^2.$$

El primer miembro es una suma de 12 cuartas potencias. Esto, con el Teorema 5.6, demuestra que todo número de la forma $6m^2$ es una suma de 12 cuartas potencias. Pero el Teorema 5.6 también demuestra que todo entero positivo de la forma $6l$ puede expresarse como una suma de cuatro números de la forma $6m^2$ y, por tanto, como una suma de 48 cuartas potencias.

Además, los enteros $j = 0, 1, 2, 81, 16, 17$ forman un sistema completo de residuos módulo 6 y cada uno es la suma de cuando más 2 cuartas potencias. Entonces todo entero $n > 81$ puede escribirse en la forma $6l + j$ con $l$ positivo y de aquí que pueda expresarse como una suma de cuando más 50 cuartas potencias. Para $0 < n \leqq 50$ se tiene $n = \sum_{i=1}^{n} 1^4$ y para $50 < n \leqq 81$ se tiene $n = 2^4 + 2^4 + 2^4 + \sum_{i=1}^{n-48} 1^4$. En todos los casos $n$ se expresa como una suma de cuando más 50 cuartas potencias.

## 5.10 Suma de dos cuadrados

No todo entero positivo es una suma de dos cuadrados. Se determinará precisamente cuáles enteros son sumas de dos cuadrados y se encontrará el número de soluciones de $x^2 + y^2 = n$.

Una solución $x, y$ de $x^2 + y^2 = n$ se llamará primitiva si $(x, y) = 1$. Restringiremos a $n$ a que sea positivo y consideraremos que

$N(n)$ = número de soluciones de $x^2 + y^2 = n$,
$P(n)$ = número de soluciones primitivas, no negativas de $x^2 + y^2 = n$,
$Q(n)$ = número de soluciones primitivas de $x^2 + y^2 = n$.

Al contar las soluciones consideraremos $x_1$, $y_1$ y $x_2$, $y_2$ como distintas si $x_1 \neq x_2$ o bien $y_1 \neq y_2$. Puede notarse que, para $n > 1$, $P(n)$ realmente es el número de soluciones primitivas positivas de $x^2 + y^2 = n$ dado que ni $x$ ni $y$ pueden ser cero.

**Teorema 5.7** *Se tiene* $N(1) = Q(1) = 4$, $P(1) = 2$ *y para* $n > 1$, $Q(n) = 4P(n)$ *y*

$$N(n) = \sum_{d^2|n} Q\left(\frac{n}{d^2}\right).$$

*Demostración.* Dado que $1 = (\pm 1)^2 + 0^2 = 0^2 + (\pm 1)^2$ y no hay otras soluciones, se tiene $N(1) = Q(1) = 4$ y $P(1) = 2$.

Si $n > 1$ y $x, y$ es una solución primitiva no negativa, entonces $x \geqq 1$, $y \geqq 1$ y $\pm x$, $\pm y$ es una solución primitiva para todas las selecciones de los signos. Con base en esto se deduce que $Q(n) = 4P(n)$.

Si $x, y$ es cualquier solución de $x^2 + y^2 = n$ y si $g = (x, y)$, entonces $g^2|n$, $(x/g, y/g) = 1$ y $(x/g)^2 + (y/g)^2 = n/g^2$. De esto es fácil ver que

$$N(n) = \sum_{d^2|n} Q\left(\frac{n}{d^2}\right).$$

**Teorema 5.8** *Supóngase que* $n > 1$. *Cada solución primitiva no negativa de* $x^2 + y^2 = n$ *determina un* $s$ *único módulo* $n$ *tal que* $sy \equiv x$

(mod $n$). *Además* $s^2 \equiv -1 \pmod{n}$ *y soluciones primitivas no negativas diferentes determinan diferente* $s$ *módulo* $n$.

*Demostración.* Si $x, y$ es una solución primitiva no negativa, entonces $(y, n) = 1$ y de aquí que $sy \equiv x \pmod{n}$ determina un $s$ único módulo $n$. Además si $y'$ es una solución de $yy' \equiv 1 \pmod{n}$, entonces $s \equiv xy' \pmod{n}$ y se tiene $s^2 \equiv x^2y'^2 \equiv -y^2y'^2 \equiv -1 \pmod{n}$.

Aun debe demostrarse que soluciones diferentes determinan diferente $s$. Supóngase que tanto $x, y$ como $u, v$ son soluciones primitivas no negativas y que $sy \equiv x \pmod{n}$ y $sv \equiv u \pmod{n}$. Entonces se tiene $xv \equiv syv \equiv yu \pmod{n}$. Pero supuesto que $n > 1$, toda solución primitiva no negativa es una solución positiva y así se tiene $1 \leqq x < \sqrt{n}$, $1 \leqq v < \sqrt{n}$. De aquí que $1 \leqq xv < n$ y de modo semejante $y \leqq yu < n$. Por tanto $xv = yu$ y de aquí que $x = u$, $y = v$, dado que $(x, y) = (u, v) = 1$ y todos los números son positivos.

**Teorema 5.9** *Supóngase que* $n > 1$, $s^2 \equiv -1 \pmod{n}$. *Existe una solución primitiva no negativa* $x, y$ *de* $x^2 + y^2 = n$ *tal que* $sy \equiv x \pmod{n}$.

*Demostración.* Considérese el conjunto de enteros $u - sv$ donde $u$ y $v$ recorren todos los valores enteros tales que $0 \leqq u \leqq \sqrt{n}$, $0 \leqq v \leqq \sqrt{n}$. Existen $(1 + [\sqrt{n}])^2 > n$ pares diferentes $u, v$. Por lo tanto, hay dos pares $u_1, v_1$ y $u_2, v_2$ tales que $u_1 - sv_1 \equiv u_2 - sv_2 \pmod{n}$. Hagamos $v_2 - v_1 = v_0$, $u_2 - u_1 = u_0$. Entonces se tiene $sv_0 \equiv u_0 \pmod{n}$ y $|u_0| \leqq \sqrt{n}$, $|v_0| \leqq \sqrt{n}$. Además, dado que $u_1, v_1$ y $u_2, v_2$ son pares diferentes, $u_0$ y $v_0$ no pueden ser ambos cero. También, puede demostrarse que por lo menos uno de $|u_0|$ y $|v_0|$ es menor que $\sqrt{n}$. Esto es obvio si $n$ no es un cuadrado. Si $n$ es un cuadrado y $|u_0| = |v_0| = \sqrt{n}$ se tiene $s\sqrt{n} \equiv \pm\sqrt{n} \pmod{n}$ y de aquí que $s \equiv \pm 1 \pmod{\sqrt{n}}$, $s^2 \equiv 1 \pmod{\sqrt{n}}$. Pero $s^2 \equiv -1 \pmod{n}$, así que se tiene $s^2 \equiv -1 \pmod{\sqrt{n}}$ y, por tanto, $1 \equiv -1 \pmod{\sqrt{n}}$. De donde $\sqrt{n} = 2$ y $n = 4$, pero esto no puede ocurrir ya que no hay entero $s$ tal que $s^2 \equiv -1 \pmod{4}$.

Las cotas para $u_0$ y $v_0$ implican la desigualdad $1 < u_0^2 + v_0^2 < 2n$. La congruencia $sv_0 \equiv u_0 \pmod{n}$ implica $u_0^2 + v_0^2 \equiv s^2v_0^2 + v_0^2 \equiv v_0^2(s^2 + 1) \equiv 0 \pmod{n}$. Todo esto implica $u_0^2 + v_0^2 = n$.

Ahora bien, sea $g = (u_0, v_0)$. Entonces $g^2 | n$ y $s(v_0/g) \equiv (u_0/g) \pmod{n/g}$, y de donde

$$\frac{n}{g^2} = \frac{u_0^2 + v_0^2}{g^2} \equiv \left(s\frac{v_0}{g}\right)^2 + \left(\frac{v_0}{g}\right)^2 \equiv -\left(\frac{v_0}{g}\right)^2 + \left(\frac{v_0}{g}\right)^2 \equiv 0 \left(\text{mód } \frac{n}{g}\right)$$

Esto es posible solamente si $g = 1$ y se tiene $(u_0, v_0) = 1$.

Finalmente, si $u_0$ y $v_0$ tienen el mismo signo hagamos $x = |u_0|$, $y = |v_0|$. Si $u_0$ y $v_0$ tienen signos opuestos hagamos $x = |v_0|$, $y = |v_0|$. En ambos casos se ve que $x, y$ es una solución primitiva no negativa. En el primer caso se tiene $sy \equiv s(\pm v_0) \equiv \pm u_0 \equiv x \pmod n$. En el segundo caso se tiene $sy \equiv s(\pm u_0) \equiv \pm s(sv_0) \equiv \mp v_0 \equiv x \pmod n$.

Los dos últimos teoremas demuestran que hay una correspondencia biunívoca entre las soluciones primitivas no negativas de $x^2 + y^2 = n$ y las soluciones de la congruencia $s^2 \equiv -1 \pmod n$. Combinando esto con el Teorema 5.7 se tiene lo siguiente.

**Teorema 5.10** *Denotemos por $R(n)$ el número de raíces de $s^2 \equiv -1 \pmod n$. Entonces $P(n) = R(n)$ para $n > 1$, $P(1) = 2$, $R(1) = 1$, $Q(1) = 4$, $Q(n) = 4R(n)$ para $n \geqq 1$ y $N(n) = 4 \sum_{d^2|n} R(n/d^2)$.*

**Teorema 5.11** *Las funciones $R(n)$ y $N(n)/4$ son funciones multiplicativas.*

*Demostración.* El hecho de que $R(n)$ es multiplicativa se deduce directamente del Teorema 2.14. Para demostrar que $N(n)/4$ es multiplicativa consideremos dos enteros cualesquiera $n_1$ y $n_2$ positivos relativamente primos. Entonces

$$\frac{1}{4} N(n_1 n_2) = \sum_{d^2|n_1 n_2} R\left(\frac{n_1 n_2}{d^2}\right) = \sum_{d_1^2|n_1} \sum_{d_2^2|n_2} R\left(\frac{n_1}{d_1^2}\frac{n_2}{d_2^2}\right)$$

$$= \sum_{d_1^2|n_1} \sum_{d_2^2|n_2} R\left(\frac{n_1}{d_1^2}\right) R\left(\frac{n_2}{d_2^2}\right) = \sum_{d_1^2|n_1} R\left(\frac{n_1}{d_1^2}\right) \sum_{d_2^2|n_2} R\left(\frac{n_2}{d_2^2}\right)$$

$$= \frac{1}{4} N(n_1) \frac{1}{4} N(n_2).$$

**Teorema 5.12** *Sean $h(1) = 1$, $h(2^e) = 0$, $h(p^e) = (-1)^{\{(p-1)/2\}e}$, $p$ un primo impar, $e \geqq 1$. Supóngase que $h(n)$ está determinada, para un $n$ compuesto en tal forma que $h(n)$ es una función multiplicativa. Entonces $N(n) = 4 \sum_{d|n} h(d)$.*

*Demostración.* Es interesante hacer notar que $h(n)$, tal y como se definió en el enunciado del teorema, en realidad es totalmente multiplicativa.

Por el teorema 4.4, $\sum_{d|n} h(d)$ es multiplicativa. Dado que $N(n)/4$ también es multiplicativa, solamente debe verificarse que $N(n) = 4 \sum_{d|n} h(d)$ para $n$ una potencia prima. La congruencia $s^2 \equiv -1 \pmod 2$ tiene la única solución $s \equiv 1 \pmod 2$. Para $e > 1$ la congruencia $s^2 \equiv -1$

(mod $2^e$) no tiene soluciones dado que $s^2 \equiv -1 \pmod 4$ no tiene. Por tanto, por el Teorema 5.10,

$$N(2^e) = 4 \sum_{f=0}^{[e/2]} R(2^{e-2f}) = 4$$

ya que no se tendrán términos diferentes de cero sólo para $e - 2f = 0$ o bien 1. De manera correspondiente se tiene

$$4 \sum_{d|2^e} h(d) = 4 \sum_{f=0}^{e} h(2^f) = 4h(1) = 4.$$

Ahora considérese un primo impar $p$. Basándose en el Teorema 2.11 se ve que $s^2 \equiv -1 \pmod p$ tiene dos soluciones si $p \equiv 1 \pmod 4$ y no tiene soluciones si $p \equiv 3 \pmod 4$. Apliquemos la Sección 2.6 al polinomio $f(x) = x^2 + 1$ con $f'(x) = 2x$. Ya que $(2s, p) = 1$, se encuentra que $s^2 \equiv -1 \pmod{p^e}$ tiene el mismo número de soluciones para todo $e \geqq 1$. Esto es

$$R(p^e) = R(p) = \begin{cases} 2 \text{ si } p \equiv 1 \pmod 4 \\ 0 \text{ si } p \equiv 3 \pmod 4, \end{cases} \qquad e \geqq 1.$$

Entonces, por el Teorema 5.10, si $e$ es par se tiene

$$(5.11) \qquad N(p^e) = 4 \sum_{f=0}^{e/2} R(p^{e-2f}) = 4 \frac{e}{2} R(p) + 4R(1)$$

$$= \begin{cases} 4e + 4 \text{ si } p \equiv 1 \ (\text{mód } 4) \\ 4 \qquad\quad \text{si } p \equiv 3 \ (\text{mód } 4), \end{cases}$$

y si $e$ es impar se tiene

$$(5.12) \qquad N(p^e) = 4 \sum_{f=0}^{(e-1)/2} R(p^{e-2f}) = 4 \frac{e+1}{2} R(p)$$

$$= \begin{cases} 4e + 4 \text{ si } p \equiv 1 \ (\text{mód } 4) \\ 0 \qquad\quad \text{si } p \equiv 3 \ (\text{mód } 4). \end{cases}$$

Correspondiendo a esto también se tiene

$$(5.13) \quad 4 \sum_{d|p^e} h(d) = 4 \sum_{f=0}^{e} h(p^f) = 4h(1) + 4 \sum_{f=1}^{e} (-1)^{\{(p-1)/2\}f}$$

$$= \begin{cases} 4 + 4e \text{ si } p \equiv 1 \ (\text{mód } 4) \\ 4 \qquad\quad \text{si } p \equiv 3 \ (\text{mód } 4), e \text{ par} \\ 0 \qquad\quad \text{si } p \equiv 3 \ (\text{mód } 4), e \text{ non} \end{cases}$$

Una comparación de (5.11) y (5.12) con (5.13) completa la demostración del teorema.

**Corolario 5.13** *$N(n)$ es cuatro veces el exceso del número de divisores de $n$ de la forma $4j + 1$ sobre aquellos de la forma $4j + 3$.*

*Demostración.* Si $d = 1$, entonces $h(d) = 1$. Si $d$ es par, entonces $h(d) = 0$. Si $d$ es impar y $d$ es el producto de los primos $p_1, p_2 \cdots, p_k$, no necesariamente distintos, entonces $h(d) = 1$ o bien $-1$ de acuerdo con que un número par o bien impar de los $p_i$ sea de la forma $4j + 3$. Pero también, en este caso, $d \equiv p_1 p_2 \cdots p_k \equiv 1$ o bien $3 \pmod 4$, de acuerdo con que un número par o bien impar de los $p_i$ sea de la forma $4j + 3$. Ya que $N(n) = 4 \sum_{d|n} h(d)$, se deduce el corolario.

**Corolario 5.14** *La ecuación $x^2 + y^2 = n$ es resoluble si, y solamente si la factorización canónica de $n$ en potencias primas no contiene factor $p^e$ con $p$ de la forma $4j + 3$ y $e$ impar.*

*Demostración.* Esto se concluye inmediatamente de (5.11) y (5.12) y el Teorema 5.11.

**Problemas**

1. Evaluar $N(n)$, $P(n)$ y $Q(n)$ para $n = 100$, 101 y 102.
2. Probar que si $n$ es exento de cuadrados, $N(n) = Q(n)$.
3. Probar que el número de representaciones de un entero $m > 1$ como una suma de dos cuadrados de enteros positivos relativamente primos es igual al número de soluciones de la congruencia $x^2 \equiv -1 \pmod m$.
4. El Corolario 5.13 implica que todo entero positivo tiene por lo menos tantos divisores de la forma $4j + 1$ como de la forma $4j + 3$. Probar este hecho directamente.
5. Para un entero positivo dado $K$, probar que existe un entero $n$ tal que
   *a*) $N(n) = K$ si, y solamente si, $K \equiv 0 \pmod 4$;
   *b*) $P(n) = K$ si, y solamente si, $K$ tiene la forma $2^m$ con $m \geq 0$;
   *c*) $Q(n) = K$ si, y solamente si, $K$ tiene la forma $2^m$ con $m \geq 2$.
6. Probar que si un entero $n$ es divisible entre un primo de la forma $4k + 3$, entonces $Q(n) = 0$.
7. Supóngase que $q$ es cualquier divisor positivo de $n$ y que $n$ es expresable como $n = a^2 + b^2$ con $(a, b) = 1$. Probar que existen los enteros $c$ y $d$ tales que $c^2 + d^2 = q$ con $(c, d) = 1$.

## 5.11 La ecuación $4x^2 + y^2 = n$

Las ideas y los métodos de la Sección 5.10 pueden extenderse ampliamente. La forma cuadrática $x^2 + y^2$ es solamente un caso especial de una teoría extendida. Sin embargo, probablemente es el caso más inte-

resante, y no haremos más que considerar unas cuantas consecuencias y aplicaciones directas.

En esta sección restringiremos nuestra atención a un positivo $n \equiv 1 \pmod 4$. Si $x^2 + y^2 = n$, entonces uno de $x$ y $y$ es impar, el otro es par. Si $x$ es par, hagamos $u = x/2$, $v = y$; si $y$ es par, hagamos $u = y/2$, $v = x$. En ambos casos se tiene $4u^2 + v^2 = n$. Dado que $x^2 + y^2 = y^2 + x^2$ y $x \neq y$, se ve que exactamente dos soluciones de $x^2 + y^2 = n$ corresponden a una solución de $4u^2 + v^2 = n$. También $(x, y) = (2u, v) = (u, v)$ ya que $v$ es impar. Si se definen $N'(n)$, $P'(n)$, $Q'(n)$ para la ecuación $4x^2 + y^2 = n$, precisamente como se definen $N(n)$, $P(n)$, $Q(n)$ para $x^2 + y^2 = n$, se tiene

$$N'(n) = \frac{N(n)}{2}, \quad P'(n) = \frac{P(n)}{2}, \quad Q'(n) = \frac{Q(n)}{2}.$$

**Teorema 5.15** *Sea un entero $n$, $n > 1$, $n \equiv 1 \pmod 4$. Si $n$ es primo, entonces $4x^2 + y^2 = n$ tiene exactamente una solución no negativa y es una solución primitiva. Si $n$ no es primo, entonces $4x^2 + y^2 = n$ tiene soluciones no primitivas, más que una solución primitiva no negativa, o bien tiene una solución primitiva no negativa y, por lo menos, una solución no primitiva no negativa.*

*Demostración.* Si $n$ es primo, usamos los Teoremas 5.12 y 5.10 para obtener

$$N'(n) = \frac{N(n)}{2} = 2(h(n) + h(1)) = 4, \qquad P'(n) = \frac{P(n)}{2} = \frac{R(n)}{2} = 1.$$

Por tanto, $4x^2 + y^2 = n$ tiene precisamente una solución primitiva no negativa, digamos $u$, $v$. Entonces, cambiando los signos de $u$ y $v$ se encuentran otras tres soluciones. Ya que $N'(n) = 4$ se ve que $4x^2 + y^2 = n$ tiene precisamente una solución no negativa y es primitiva.

Si $n$ es compuesto y si algún primo $p \equiv 3 \pmod 4$ divide a $n$, entonces, por el Teorema 5.10, $Q'(n) = Q(n)/2 = 2R(n) = 0$. De donde $4x^2 + y^2 = n$ no tiene soluciones primitivas en este caso.

Si $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, $p_i \equiv 1 \pmod 4$, $e_i > 0$, $r > 1$, entonces $P'(n) = P(n)/2 = R(n)/2 = 2^{r-1} > 1$ y $4x^2 + y^2 = n$ tiene más de una solución primitiva no negativa.

Si $n = p^e$, $e > 1$, $p \equiv 1 \pmod 4$, entonces

$$N'(n) = \frac{N(n)}{2} = 2 \sum_{f=0}^{e} h(p^f) = 2(e+1) \geqq 6$$

y $P'(n) = P(n)/2 = R(p^e)/2 = 1$. Por lo tanto, $4x^2 + y^2 = n$ tiene precisamente una solución primitiva no negativa y tiene más de cuatro soluciones. Debe tener alguna solución no primitiva $u$, $v$. Entonces

$|u|$, $|v|$ es una solución no primitiva no negativa. Esto completa la demostración.

El problema de decidir si algún número es primo o no, siempre ha sido interesante para muchos. Si el número es grande puede ser un verdadero problema y esto ha conducido al desarrollo de varios métodos y máquinas. No importa qué tan lejos se haya llegado, siempre hay alguien tratando de llegar un poco más adelante. El Teorema 5.15 es un criterio respecto a la condición de primo. Dado $n \equiv 1 \pmod 4$, se buscan las soluciones no negativas de $4x^2 + y^2 = n$. Si se encuentra una solución no primitiva o dos soluciones no negativas, ya no es necesario seguir adelante; $n$ es compuesto. Si no hay soluciones, nuevamente $n$ es compuesto. Si hay exactamente una solución no negativa, será primitiva, y $n$ es primo.

Si se encuentra una solución no primitiva $x$, $y$ de $4x^2 + y^2 = n$ no solamente se sabe que $n$ es compuesto sino que también se conoce un factor $(x, y)$ de $n$. Si se encuentran dos soluciones primitivas no negativas $u$, $v$ y $\mu$, $\nu$ también puede encontrarse un factor de $n$. Dado que $2u$, $v$ y $2\mu$, $\nu$ son soluciones primitivas no negativas diferentes de $x^2 + y^2 = n$, determinan diferentes $s$ y $t$ tales que $sv \equiv 2u \pmod n$, $t\nu \equiv 2\mu \pmod n$, por el Teorema 5.8. Entonces $s^2 \equiv t^2 \equiv -1 \pmod n$, $s \not\equiv t \pmod n$,

$$\text{y} \quad 2(s-t)(u\nu + v\mu) \equiv (s-t)(sv\nu + vt\nu) \equiv (s-t)(s+t)v\nu$$
$$\equiv (s^2 - t^2)v\nu \equiv 0 \pmod n,$$

lo cual implica que $u\nu + v\mu$ y $n$ tiene un factor común $> 1$. Si $g$ denota a $(u\nu + v\mu, n)$ entonces

$$1 < g \leqq u\nu + v\mu \leqq \left[\frac{\sqrt{n}}{2}\right][\sqrt{n}] + \left[\frac{\sqrt{n}}{2}\right][\sqrt{n}] < n,$$

y $g$ es un factor propio de $n$.

Cuando se buscan las soluciones no negativas de $4x^2 + y^2 = n$, puede restringirse $x$ a $0 \leqq x \leqq \sqrt{n}/2$ y solamente se necesita comprobar si $n - 4x^2$ es un cuadrado perfecto. Pero incluso no es necesario probar todos estos valores de $x$. Supuesto que $y$ es impar, se tiene $y^2 \equiv 1 \pmod 8$. Por tanto, $x$ debe satisfacer $n - 4x^2 \equiv 1 \pmod 8$, lo cual es equivalente a $x^2 \equiv (n-1)/4 \pmod 2$. De donde, $x$ es par si $n \equiv 1 \pmod 8$, $x$ es impar si $n \equiv 5 \pmod 8$. En cualquier caso, debe dividirse a la mitad el número de $x$ que deben probarse.

Yendo más adelante, si $c$ es impar y positivo entonces $n - 4x^2 \equiv y^2 \pmod c$ y puede excluirse todo $x$ para el cual $n - 4x^2$ es un no residuo cuadrático módulo $c$. Por ejemplo, 2 y 3 son no residuos módulo 5 y puede excluirse $x$ para el cual $n - 4x^2 \equiv 2$ o bien $3 \pmod 5$, esto es $x^2 \equiv 2 - n$ o bien $3 - n \pmod 5$. Si $n \equiv 3 \pmod 5$ esto excluye al $x$ tal que $x^2 \equiv -1$ o bien $0 \pmod 5$, es decir $x \equiv 0, 2, 3 \pmod 5$.

Considérese un ejemplo sencillo. Tomemos $n = 4993$. Entonces puede restringirse $x$ a $0 \leqq x < 71/2 < 36$. Dado que $n \equiv 1 \pmod 8$, tomemos $x$ par. Ya que $n \equiv 3 \pmod 5$ pueden excluirse todos los $x \equiv 0$, 2, 3 (mod 5). Escribiendo los números pares 0, 2, 4, . . . , 34 y cancelando los $x \equiv 0, 2, 3 \pmod 5$ se encuentra que sólo es necesario probar $x = 4, 6, 14, 16, 24, 26, 34$. Esta lista puede acortarse aún más si se usan otros valores de $c$. Por ejemplo $c = 7$ elimina 6 y 34, y $c = 11$ elimina 14. Esto apenas vale la pena para un $n$ de este tamaño. En cualquier caso sólo se tiene que comprobar unos cuantos valores. Se encontrará que $x = 16$ da $n - 4x^2 = 3969 = 63^2$ y que no hay otras soluciones. Por tanto, 4993 es primo.

Probablemente, para valores mayores de $n$ se usarían más valores de $c$. Si fuera necesario usar muchas veces este método, sería recomendable construir pequeñas tablas que muestren cuáles $x$ se excluyen para varios valores de $c$. Si el método se lleva a cabo sistemáticamente, y si se tiene disponible una tabla de cuadrados, es una prueba útil respecto a la condición de primo de $n$ que no sea demasiado grande. Esta prueba se basó en la ecuación $4x^2 + y^2 = n$ y solamente es útil para $n \equiv 1$ (mod 4). Existen otras pruebas, basadas en otras ecuaciones, válidas para otros $n$.

## 5.12 La ecuación $ax^2 + by^2 + cz^2 = 0$

Aunque el teorema que se da referente a esta ecuación data desde Legendre, la demostración es reciente (ver la bibliografía al final del libro).

**Teorema 5.16** *Sean a, b, c enteros diferentes de cero tales que el producto abc es exento de cuadrados. Las condiciones necesarias y suficientes para que* $ax^2 + by^2 + cz^2 = 0$ *tenga una solución en los enteros x, y, z, no todos cero, son que a, b, c no tengan el mismo signo y que* $-bc$, $-ac$, $-ab$ *sean residuos cuadráticos módulo a, b, c, respectivamente.*

Antes de dar la demostración de este resultado estableceremos dos lemas.

**Lema 5.17** *Sean* $\lambda$, $\mu$, $\nu$ *números positivos reales con producto entero* $\lambda\mu\nu = m$. *Entonces cualquier congruencia* $\alpha x + \beta y + \gamma z \equiv 0 \pmod m$ *tiene una solución x, y, z, no todos cero, tal que* $|x| \leqq \lambda$, $|y| \leqq \mu$, $|z| \leqq \nu$.

*Demostración.* Supóngase que $x$ recorre los valores $0, 1, \ldots, [\lambda]$, $y$ recorre $0, 1, \ldots, [\mu]$ y $z$ recorre $0, 1, \ldots, [\nu]$. Esto proporciona $(1 + [\lambda])(1 + [\mu])(1 + [\nu])$ tripletas diferentes $x, y, z$. Ahora bien, por

el Teorema 4.1$a$, $(1 + [\lambda])(1 + [\mu])(1 + [\nu]) > \lambda\mu\nu = m$, de donde deben existir dos tripletas $x_1, y_1, z_1$ y $x_2, y_2, z_2$ tales que $\alpha x_1 + \beta y_1 + \gamma z_1 \equiv \alpha x_2 + \beta y_2 + \gamma z_2 \pmod{m}$. Entonces se tiene $\alpha(x_1 - x_2) + \beta(y_1 - y_2) + \gamma(z_1 - z_2) \equiv 0 \pmod{m}$, $|x_1 - x_2| \leqq [\lambda] \leqq \lambda$, $|y_1 - y_2| \leqq \mu$, $|z_1 - z_2| \leqq \nu$.

**Lema 5.18** *Supóngase que $ax^2 + by^2 + cz^2$ se factoriza en factores lineales módulo $m$ y también módulo $n$; esto es*

$$ax^2 + by^2 + cz^2 \equiv (\alpha_1 x + \beta_1 y + \gamma_1 z)(\alpha_2 x + \beta_2 y + \gamma_2 z) \pmod{m},$$
$$ax^2 + by^2 + cz^2 \equiv (\alpha_3 x + \beta_3 y + \gamma_3 z)(\alpha_4 x + \beta_4 y + \gamma_4 z) \pmod{n},$$

*Si $(m, n) = 1$ entonces $ax^2 + by^2 + cz^2$ se factoriza en factores lineales módulo $mn$.*

*Demostración.* Aplicando el Teorema 2.14, pueden escogerse $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ para satisfacer

$$\alpha \equiv \alpha_1, \beta \equiv \beta_1, \gamma \equiv \gamma_1, \alpha' \equiv \alpha_2, \beta' \equiv \beta_2, \gamma' \equiv \gamma_2 \pmod{m},$$
$$\alpha \equiv \alpha_3, \beta \equiv \beta_3, \gamma \equiv \gamma_3, \alpha' \equiv \alpha_4, \beta' \equiv \beta_4, \gamma' \equiv \gamma_4 \pmod{n}.$$

Entonces la congruencia

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z)$$

se cumple para el módulo $m$ y el módulo $n$ y de aquí que se cumple para el módulo $mn$.

*Demostración del Teorema* 5.16. Si $ax^2 + by^2 + cz^2 = 0$ tiene una solución $x_0, y_0, z_0$, no todos cero, entonces $a, b, c$ no son del mismo signo. Dividiendo $x_0, y_0, z_0$ entre $(x_0, y_0, z_0)$ se tiene una solución $x_1, y_1, z_1$ con $(x_1, y_1, z_1) = 1$.

Ahora se probará que $(c, x_1) = 1$. Si no fuera así habría un primo $p$ que dividirá tanto a $c$ como a $x_1$. Entonces $p \nmid b$ dado que $p|c$ y $abc$ son exentos de cuadrados. Por tanto, $p|by_1^2$ y $p \nmid b$, de donde $p|y_1^2$, $p|y_1$ y, entonces, $p^2|(ax_1^2 + by_1^2)$ de modo que $p^2|cz_1^2$. Pero $c$ es exento de cuadrados de manera que $p|z_1$. Se ha concluido que $p$ es un factor de $x_1$, $y_1$ y $z_1$ lo cual es contrario al hecho de que $(x_1, y_1, z_1) = 1$. En consecuencia, se tiene $(c, x_1) = 1$.

Escójase $u$ de manera que satisfaga $ux_1 \equiv 1 \pmod{c}$. Entonces la ecuación $ax_1^2 + by_1^2 + cz_1^2 = 0$ implica $ax_1^2 + by_1^2 \equiv 0 \pmod{c}$ y multiplicando esto por $u^2b$ se obtiene $u^2b^2y_1^2 \equiv -ab \pmod{c}$. Así se ha establecido que $-ab$ es un residuo cuadrático módulo $c$. Una demostración semejante demuestra que $-bc$ y $-ac$ son residuos cuadráticos módulo $a$ y $b$, respectivamente.

Inversamente, supongamos que $-bc, -ac, -ab$ son residuos cuadráticos módulo $a, b, c$, respectivamente. Nótese que esta propiedad no

cambia si $a, b, c$ se remplazan por sus negativos. Dado que $a, b, c$ no son del mismo signo, pueden cambiarse los signos de todos ellos, si es necesario, para tener uno de ellos positivo y los otros dos negativos. Entonces tal vez con un cambio de notación, pueda arreglarse de manera que $a$ sea positivo y $b$ y $c$ negativos.

Definir $r$ como una solución de $r^2 \equiv -ab \pmod{c}$ y $a_1$ como una solución de $aa_1 \equiv 1 \pmod{c}$. Estas soluciones existen debido a las suposiciones acerca de $a, b, c$. Entonces puede escribirse

$$ax^2 + by^2 \equiv aa_1(ax^2 + by^2) \equiv a_1(a^2x^2 + aby^2) \equiv a_1(a^2x^2 - r^2y^2)$$
$$\equiv a_1(ax - ry)(ax + ry) \equiv (x - a_1ry)(ax + ry) \pmod{c},$$
$$ax^2 + by^2 + cz^2 \equiv (x - a_1ry)(ax + ry) \pmod{c}.$$

Así que $ax^2 + by^2 + cz^2$ es el producto de dos factores lineales módulo $c$ y, de modo semejante, módulo $a$ y módulo $b$. Aplicando el Lema 5.18 dos veces, se concluye que $ax^2 + by^2 + cz^2$ puede escribirse como el producto de dos factores lineales módulo $abc$. Es decir, existen los números $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$ tales que

$$(5.14)\quad ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z) \pmod{abc}.$$

Ahora apliquemos el Lema 5.17 a la congruencia

$$(5.15)\qquad \alpha x + \beta y + \gamma z \equiv 0 \pmod{abc},$$

usando $\lambda = \sqrt{bc}$, $\mu = \sqrt{|ac|}$, $\nu = \sqrt{|ab|}$. Así se obtiene una solución $x_1, y_1, z_1$ de la congruencia (5.15) con $|x_1| \leqq \sqrt{bc}$, $|y_1| \leqq \sqrt{|ac|}$, $|z_1| \leqq \sqrt{|ab|}$. Pero $abc$ es exento de cuadrados, de manera que $\sqrt{bc}$ es un entero solamente si es 1 y del mismo modo para $\sqrt{|ac|}$ y $\sqrt{|ab|}$. De donde se tiene

$|x_1| \leqq \sqrt{bc}$, $x_1^2 \leqq bc$ con igualdad posible sólo si $b = c = -1$;

$|y_1| \leqq \sqrt{|ac|}$, $y_1^2 \leqq -ac$ con igualdad posible sólo si $a = 1$, $c = -1$,

$|z_1| \leqq \sqrt{|ab|}$, $z_1^2 \leqq -ab$ con igualdad posible sólo si $a = 1$, $b = -1$.

De aquí que, dado que $a$ es positivo y $b$ y $c$ son negativos, se tiene, a menos que $b = c = -1$,

$$ax_1^2 + by_1^2 + cz_1^2 \leqq ax_1^2 < abc,$$

y

$$ax_1^2 + by_1^2 + cz_1^2 \geqq by_1^2 + cz_1^2 > b(-ac) + c(-ab) = -2abc.$$

Dejando a un lado el caso especial cuando $b = c = -1$, se tiene

$$-2abc < ax_1^2 + by_1^2 + cz_1^2 < abc.$$

Ahora bien, $x_1, y_1, z_1$ es una solución de (5.15) y, debido a (5.14), también lo es de

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{abc}.$$

Por lo tanto, las desigualdades anteriores implican que

$$ax_1^2 + by_1^2 + cz_1^2 = 0 \quad \text{o bien} \quad ax_1^2 + by_1^2 + cz_1^2 = -abc.$$

En el primer caso se tiene nuestra solución de $ax^2 + by^2 + cz^2 = 0$. En el segundo caso rápidamente se verifica que $x_2, y_2, z_2$ definidos por $x_2 = -by_1 + x_1z_1, y_2 = ax_1 + y_1z_1, z_2 = z_1^2 + ab$, forman una solución. En el caso de que $x_2 = y_2 = z_2 = 0$ fácilmente se encuentra una solución propia.

Finalmente debe tomarse en cuenta el caso especial $b = c = -1$. Las condiciones sobre $a, b, c$ ahora implican que $-1$ es un residuo cuadrático módulo $a$, en otras palabras, que $R(a)$ del Teorema 5.10 es positiva. Por el Teorema 5.10, esto implica que $Q(a)$ es positiva y de aquí que la ecuación $y^2 + z^2 = a$ tiene una solución $y_1, z_1$. Entonces $x = 1, y = y_1, z = z_1$ es una solución de $ax^2 + by^2 + cz^2 = 0$ supuesto que $b = c = -1$.

**Problema**

1. Demostrar que en la prueba del Teorema 5.16 se ha establecido más de lo que enuncia el teorema, que se implica el siguiente resultado más fuerte. Sean $a, b, c$ enteros diferentes de cero no del mismo signo tales que el producto $abc$ es exento de cuadrados. Entonces son equivalentes las tres condiciones siguientes.
   *a*) $ax^2 + by^2 + cz^2 = 0$ tiene una solución $x, y, z$ no todos cero;
   *b*) $ax^2 + by^2 + cz^2$ se factoriza en factores lineales módulo $abc$;
   *c*) $-bc, -ac, -ab$ son residuos cuadráticos módulo $a, b, c$, respectivamente.

## 5.13 Formas cuadráticas binarias

Una forma es un polinomio homogéneo, esto es, un polinomio en varias variables, cuyos términos todos son del mismo grado. Una forma cuadrática $f$ tiene términos de grado dos y, por lo tanto, es una expresión del tipo

$$(5.16) \qquad f(x_1, x_2, \cdots, x_n) = \sum_{i,j=1}^{n} a_{ij}x_ix_j.$$

Restringiremos nuestra atención a las formas cuadráticas con coeficientes enteros $a_{ij}$. Si $f(x_1, x_2, \cdots, x_n)$ asume solamente valores positivos siempre que $x_1, x_2, \cdots, x_n$ se reemplaza por cualquier conjunto de enteros que

no sean $0, 0, \cdots, 0$, entonces se dice que $f$ es una forma positiva. De modo semejante, $f$ es una forma negativa si su valor es negativo cuando $x_1, x_2, \cdots, x_n$ se reemplazan por enteros no todos cero. Una forma definida es aquella que es positiva o bien negativa. Por ejemplo, $x_1^2 + x_2^2$ o bien $x^2 + y^2$ en otra notación, es una forma positiva y $-x^2 - 3y^2$ es una forma negativa; ambas son formas definidas. La forma $x^2 - y^2$ es una forma indefinida. En ocasiones las formas positivas reciben el nombre de positivas definidas y las formas negativas de negativas definidas. Evidentemente, si $f$ es positiva entonces $-f$ es negativa e inversamente. De aquí que no es necesario estudiar tanto las formas positivas como las negativas debido a que las propiedades de las de un tipo se deducen de las propiedades de las otras.

Se dice que una forma cuadrática (5.16) representa un entero $m$ si existen los enteros $b_1, b_2, \cdots, b_n$ tales que $f(b_1, b_2, \cdots, b_n) = m$. Por ejemplo, $x^2 + y^2$ representa 5 pero no 6. Toda forma cuadrática representa 0 porque $f(0, 0, \cdots, 0) = 0$. La forma $f$ se llama forma cero si $f(b_1, b_2, \cdots, b_n) = 0$ para algunos enteros $b_1, b_2, \cdots, b_n$, no todos cero. Por definición, una forma definida no es una forma cero. El Teorema 5.16 dio las condiciones necesarias y suficientes para que $ax^2 + by^2 + cz^2$ sea una forma cero para una amplia clase de enteros $a, b, c$.

Se dice que una forma positiva es universal si representa todos los enteros positivos. Por tanto, de acuerdo con el Teorema 5.6, $x_1^2 + x_2^2 + x_3^2 + x_4^2$ es una forma universal. Aunque no se probará, es un hecho de que ninguna forma del tipo $ax^2 + by^2 + cz^2$ puede ser universal. La teoría aritmética de las formas cuadráticas incluye tales problemas como determinar cuáles formas son universales, determinar o bien caracterizar la clase de enteros representados por una forma cuadrática que no es universal y determinar en cuántas formas puede representarse un entero mediante una forma cuadrática. Por ejemplo, el Corolario 5.14 determinó la clase de enteros representados por la forma $x^2 + y^2$ y el Corolario 5.13 determinó el número de representaciones.

Una forma que contiene dos variables se llama forma binaria. El resto de este capítulo se referirá a las formas cuadráticas binarias, esto es, formas del tipo

$$(5.17) \qquad f(x, y) = ax^2 + bxy + cy^2.$$

No se intentará más que dar precisamente una introducción a una parte de la teoría que se refiere a las formas cuadráticas binarias. El uso de las matrices simplificaría algunas de nuestras demostraciones. No obstante, por lo poco que se hará, la simplificación no es suficiente para compensar el trabajo que requeriría la introducción de matrices.

**Teorema 5.19** *La forma cuadrática* $f(x,y) = ax^2 + bxy + cy^2$ *es positiva si y solamente si su discriminante* $b^2 - 4ac$ *es negativo,* $a > 0$ *y* $c > 0$.

*Demostración.* Dado que $f(1,0) = a$ y $f(0,1) = c$, se ve que $f$ no es positiva si $a \leqq 0$ o bien si $c \leqq 0$. Ahora puede suponerse $a > 0$, $c > 0$ y puede escribirse

$$f(x,y) = \frac{1}{4a}\left((2ax + by)^2 + (4ac - b^2)y^2\right). \tag{5.18}$$

Esto demuestra que $f(-b, 2a) = (4ac - b^2)a$ y de aquí que, supuesto que $a > 0$, que $f$ no es positiva si $4ac - b^2 \leqq 0$. Por otra parte, si $b^2 - 4ac < 0$, demuestra que $f(x,y)$ nunca es negativa sin importar qué enteros puedan sustituirse por $x$ y $y$. Aún más, entonces $f(x,y) = 0$ se cumple si, y solamente si, $2ax + by = 0$ $y$ $(4ac - b^2)y^2 = 0$. Estas ecuaciones implican que $y = 0$ y $x = 0$ si $a > 0$, $b^2 - 4ac < 0$.

La forma cuadrática $x^2 - dy^2$ con $d > 0$ tiene discriminante $4d > 0$ y evidentemente es indefinido. La ecuación de Pell $x^2 - dy^2 = n$, $d > 0$, $d$ no es un cuadrado perfecto, se discutirá en la Sección 7.8. Para $d$ y $n$ fijos resulta que la ecuación no tiene solución o bien un número infinito de soluciones. Por otra parte, es fácil ver que $x^2 - y^2 = n$ no tiene soluciones si $n \equiv 2 \pmod 4$ y solamente un número finito de soluciones, $x = (t + n/t)/2, y = (t - n/t)/2, t|n, t \equiv n \pmod 2$, si $n \not\equiv 2 \pmod 4$. La primera situación no se origina en el caso de formas definidas, como se muestra en el siguiente teorema.

**Teorema 5.20** *Sea* $f$ *una forma cuadrática positiva. Entonces el número de representaciones de un entero* $m$ *mediante* $f$ *es finito, posiblemente cero.*

*Demostración.* Se demostrará que existe solamente un número finito de pares de enteros para los cuales $f(x,y) \leqq m$. Puede suponerse $m > 0$. Aplicando (5.18) se ve que $f(x,y) \leqq m$ implica $(4ac - b^2)y^2 \leqq 4am$ y de donde

$$-2\left(\frac{am}{4ac - b^2}\right)^{1/2} \leqq y \leqq 2\left(\frac{am}{4ac - b^2}\right)^{1/2}.$$

Esto restringe $y$ a un número finito de valores. Entonces para cada una de esas $y$ se tiene $(2ax + by)^2 \leqq 4am - (4ac - b^2)y^2$, lo cual entonces restringe $2ax + by$ y de aquí a $x$ a un número finito de valores.

**Corolario 5.21** *Sea* $f$ *una forma cuadrática positiva. Entonces el menor entero positivo representado por* $f$ *puede encontrarse en un número finito de pasos.*

*Demostración.* Dado que $a$ es representado por $f$ tomemos precisamente $m = a - 1$ en la demostración del Teorema 5.20, se encuentran

todos los $y$ y $x$ permitidos y a continuación se determina el menor valor de $f(x, y)$.

Por ejemplo, si $f(x, y) = 5x^2 + 14xy + 11y^2$, entonces $b^2 - 4ac = -24 < 0$ y $y$ se limita a $-\sqrt{30}/3 \leqq y \leqq \sqrt{30}/3$. De aquí que $y = -1$, 0, 1. Para $y = -1$ se tiene $(10x - 14)^2 \leqq 56$ de lo cual se encuentra $x = 1$ o bien 2, $f(x, -1) = 2$ o bien 3. Para $y = 0$ se encuentra $x = 0$, $f(0, 0) = 0$. Para $y = 1$ se encuentra $x = -2$ o bien $-1$, $f(x, 1) = 3$ o bien 2. De donde el menor entero positivo representado por $f$ es 2.

Si en la forma cuadrática $f(x, y) = 5x^2 + 14xy + 11y^2$ se reemplaza $x$ por $-X + 2Y$ y $y$ por $X - Y$ se obtiene la forma $F(X, Y) = 2X^2 + 3Y^2$. Ahora la transformación

$$x = -X + 2Y, \qquad y = X - Y \tag{5.19}$$

puede resolverse para $X$ y $Y$ para dar la transformación inversa

$$X = x + 2y, \qquad Y = x + y.$$

La transformación (5.19) tiene la propiedad especial de que su inversa también tiene coeficientes enteros; tanto (5.19) como su inversa son transformaciones enteras. Si $X$ y $Y$ se reemplazan por enteros, entonces (5.19) da un par de enteros para $x$ y $y$ para hacer el valor de $f(x, y)$ el mismo que el de $F(X, Y)$. La transformación inversa opera en el otro camino, dando los enteros $X$ y $Y$ correspondientes a los enteros $x$ y $y$.

Se deduce que cualquier entero representado por $f$ también puede representarse por $F$ e inversamente. Además, el número de representaciones es el mismo en ambos casos. La forma $F$ es considerablemente más sencilla que la $f$. Por tanteos, es fácil verificar que todas las soluciones de $F(X, Y) = 14$ son $(1, 2)$; $(1, -2)$, $(-1, 2)$, $(-1, -2)$. Entonces (5.19) nos da las soluciones de $f(x, y) = 14$, a saber $(3, -1)$, $(-5, 3)$, $(5, -3)$, $(-3, 1)$.

Se dice que la forma cuadrática $F$ es equivalente a $f$. Todo lo que puede decirse respecto a las representaciones por $F$ puede llevarse hacia $f$ en virtud de (5.19) y su inversa. Si se estudia $F$ no es necesario estudiar $f$ o bien cualquier otra forma equivalente. Este ejemplo sugiere la conveniencia de estudiar más cuidadosamente las transformaciones y la equivalencia de formas.

**Problemas**

1. Determinar la clase de enteros representada por cada una de las siguientes formas:

   *a*) $2x^2 + 2y^2$;
   *b*) $2x^2 - 2y^2$;
   *c*) $x^2 - xy$;
   *d*) $2x^2 + 2y^2 + 2z^2 + 2t^2$.

2. Probar que $x^2 - 2xy + y^2$ es una forma cero. Determinar la clase de enteros representada por esta forma.
3. Si $C$ es cualquier clase de enteros, finita o infinita, denotemos por $mC$ la clase obtenida al multiplicar cada entero de $C$ por el entero $m$. Probar que si $C$ es la clase de enteros representada por cualquier forma $f$, entonces $mC$ es la clase representada por $mf$.
4. Probar que $ax^2 + bxy + cy^2$ es una forma positiva si, y solamente si, $a > 0$ y $b^2 - 4ac < 0$. (Observar que este problema muestra que la condición $c > 0$ del Teorema 5.19 es superflua).
5. Probar que $ax^2 + bxy + cy^2$ es una forma positiva si, y solamente si, $c > 0$ y $b^2 - 4ac < 0$.
6. Probar que la forma $ax^2 + bxy + cy^2$ es negativa si, y solamente si, $a < 0$ y $b^2 - 4ac < 0$.
7. Probar que la forma $ax^2 + bxy + cy^2$ es definida si, y solamente si, $b^2 - 4ac < 0$.
8. Probar que $x^2 + 7xy + y^2$ no es forma definida ni forma cero.
9. Encontrar todas las soluciones de las ecuaciones diofantinas.
   *a*) $5x^2 + 14xy + 11y^2 = 35$;
   *b*) $5x^2 + 14xy + 11y^2 = 46$.
10. Encontrar el menor entero positivo representado por la forma positiva $7x^2 + 25xy + 23y^2$.
11. Si $f(x, y)$ es una forma cuadrática binaria positiva, probar que $f(\alpha, \beta)$ es positiva para todo par de números reales $\alpha, \beta$, excepto $0, 0$.
12. Sea $f(x, y) = ax^2 + bxy + cy^2$ una forma cuadrática con $a > 0$ y $b^2 - 4ac = 0$. Dado también que $(a, b, c) = 1$, probar que los enteros representados por $f$ son precisamente los números $m^2$, con $m = 0, 1, 2, \cdots$. De aquí, quitando la restricción de que $(a, b, c) = 1$, probar que los enteros representados por $f$ son todos los números de la forma $dm^2$, donde $d = (a, b, c)$.

## 5.14 Equivalencia de formas cuadráticas

**Teorema 5.22** *La inversa de una transformación entera*

$$x = \alpha X + \beta Y, \qquad y = \gamma X + \delta Y \tag{5.20}$$

*es también una transformación entera si y solamente si* $\Delta = \pm 1$, *donde* $\Delta$ *es el determinante de la transformación,*

$$\Delta = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma.$$

*Demostración.* La inversa existe si y solamente si (5.20) puede resolverse unívocamente para $X$ y $Y$, de aquí que si y solamente si $\Delta \neq 0$. Entonces, si la inversa existe puede resolverse para obtener

$$X = \frac{\delta}{\Delta} x - \frac{\beta}{\Delta} y, \qquad Y = -\frac{\gamma}{\Delta} x + \frac{\alpha}{\Delta} y. \tag{5.21}$$

Si $\Delta = \pm 1$ entonces (5.21) es una tranformación entera.

Ahora supóngase que (5.21) es una transformación entera. Sea $p$ cualquier primo, y sea $p^k$ la potencia máxima de $p$ que divide a $\Delta$. Si $p$ no divide a $\Delta$, entonces $k = 0$. Dado que los coeficientes en (5.21) son enteros, se concluye que

$$p^k|\delta, \quad p^k|\beta, \quad p^k|\gamma, \quad p^k|\alpha.$$

Se deduce que

$$p^{2k}|\alpha\delta, \quad p^{2k}|\beta\gamma, \quad p^{2k}|\Delta.$$

Pero $p^k$ es la máxima potencia de $p$ que divide a $\Delta$, de modo que se tiene $2k \leqq k$, lo cual implica $k = 0$. Por tanto ningún primo divide a $\Delta$ y de donde $\Delta = \pm 1$.

Este teorema muestra que si $F$ es una forma cuadrática obtenida de una forma $f$ por medio de (5.20) con $\Delta = \pm 1$, entonces, precisamente como en la Sección 5.13, el problema de representar los enteros por $f$ puede reducirse al de representarlos mediante $F$.

**Definición 5.1** *Una forma cuadrática* $f(x, y) = ax^2 + bxy + cy^2$ *es equivalente a una forma* $g(x, y) = Ax^2 + Bxy + Cy^2$ *si existe una transformación entera* (5.20), *con determinante* $\Delta = \pm 1$, *que lleve* $f(x, y)$ *hacia* $g(X, Y)$. *En caso de que* $f$ *sea equivalente a* $g$ *se escribe* $f \sim g$.

Aplicando (5.20) a $f$ y multiplicando se encuentra

(5.22) $$A = a\alpha^2 + b\alpha\gamma + c\gamma^2, \quad B = 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta,$$
$$C = a\beta^2 + b\beta\delta + c\delta^2,$$

si (5.20) lleva $f(x, y)$ hacia $g(X, Y)$.

El siguiente teorema muestra que esta equivalencia es una verdadera relación de equivalencia: es reflexiva, simétrica y transitiva.

**Teorema 5.23** *Sean* $f$, $g$ *y* $h$ *formas cuadráticas binarias. Entonces*

*a*) $f \sim f$,
*b*) si $f \sim g$ entonces $g \sim f$,
*c*) si $f \sim g$ y $g \sim h$ entonces $f \sim h$.

*Demostración.* *a*) La transformación identidad $x = X$, $y = Y$ tiene determinante 1 y lleva $f(x, y)$ hacia $f(X, Y)$.

*b*) Puede suponerse que (5.20) es la transformación que lleva $f(x, y)$ hacia $g(X, Y)$. Entonces, por (5.21), la transformación que lleva $g(X, Y)$ nuevamente hacia $f(x, y)$ tiene determinante

$$\frac{\delta}{\Delta}\frac{\alpha}{\Delta} - \frac{\beta}{\Delta}\frac{\gamma}{\Delta} = \frac{1}{\Delta} = \pm 1.$$

*c*) Se supone que (5.20) con $\Delta = \pm 1$ lleva $f(x, y)$ hacia $g(X, Y)$ y que la transformación $X = \alpha_1 u + \beta_1 v$, $Y = \gamma_1 u + \delta_1 v$, con $\Delta_1 =$

$\alpha_1\delta_1 - \beta_1\gamma_1 = \pm 1$ lleva $g(X, Y)$ hacia $h(u, v)$. Si se eliminan $X$ y $Y$, se encuentra

$$x = (\alpha\alpha_1 + \beta\gamma_1)u + (\alpha\beta_1 + \beta\delta_1)v,$$
$$y = (\gamma\alpha_1 + \delta\gamma_1)u + (\gamma\beta_1 + \delta\delta_1)v,$$

y esta transformación lleva $f(x, y)$ hacia $h(u, v)$. Un cálculo fácil muestra que el determinante de esta transformación es igual a $(\alpha\delta - \beta\gamma)(\alpha_1\delta_1 - \beta_1\gamma_1) = \pm 1$. Por lo tanto, $f(x, y)$ es equivalente a $h(x, y)$.

**Teorema 5.24** *Si $f \sim g$, entonces los discriminantes de $f$ y $g$ son iguales.*

*Demostración.* Supongamos que (5.20) lleva $f(x, y)$ hacia $g(X, Y)$ como en la Definición 5.1. Es posible calcular el discriminante $B^2 - 4AC$ de $g$ aplicando (5.22), para obtener $B^2 - 4AC = (\alpha\delta - \beta\gamma)^2(b^2 - 4ac)$ pero es más sencillo usar la regla común para multiplicar determinantes,

$$\begin{vmatrix} \alpha & \gamma \\ \beta & \delta \end{vmatrix} \begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \begin{vmatrix} 2a\alpha + b\gamma & b\alpha + 2c\gamma \\ 2a\beta + b\delta & b\beta + 2c\delta \end{vmatrix} \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}$$
$$= \begin{vmatrix} 2A & B \\ B & 2C \end{vmatrix}.$$

Evaluando los determinantes se encuentra $(\alpha\delta - \beta\gamma)^2(4ac - b^2) = 4AC - B^2$. Dado que $(\alpha\delta - \beta\gamma)^2 = \Delta^2 = 1$ se tiene $b^2 - 4ac = B^2 - 4AC$.

A la luz del Teorema 5.23 pueden separarse todas las formas cuadráticas binarias en clases de equivalencias, poniendo dos formas $f$ y $g$ en la misma clase si $f \sim g$. La parte $(b)$ del Teorema 5.23 asegura que $f$ y $g$ representan el mismo conjunto de enteros si $f$ y $g$ están en la misma clase y que hay una correspondencia biunívoca entre las representaciones mediante $f$ y aquellas mediante $g$. En otras palabras es suficiente considerar sólo una forma representativa de cada clase de equivalencias. Evidentemente, si una forma en una clase es positiva entonces lo son todas las demás en esa clase. También dos formas en la misma clase tienen los mismos discriminantes.

La siguiente cosa que es conveniente tener es alguna manera de seleccionar una forma representativa única de cada clase de equivalencias. En el caso de las formas cuadráticas binarias positivas, esto puede hacerse de un modo bastante sencillo. La teoría completa relacionada con las formas positivas es muy elegante. Por esta razón, de ahora en adelante, restringiremos nuestra atención a las formas positivas.

**Definición 5.2** *Una forma cuadrática binaria positiva $ax^2 + bxy + cy^2$ es una forma reducida si $0 \leqq b \leqq a \leqq c$.*

Por ejemplo, $x^2 + y^2$ es una forma reducida.

**Teorema 5.25** *A cada forma cuadrática binaria positiva le corresponde una forma reducida equivalente.*

*Demostración.* Considérese cualquier forma cuadrática binaria positiva $g(x, y) = Ax^2 + Bxy + Cy^2$. Se demostrará que existe una forma equivalente $ax^2 + bxy + cy^2$ con $0 \leqq |b| \leqq a \leqq c$. Esto bastará porque en el caso de que $b$ sea negativo, la transformación $x = -X$, $y = Y$ llevará $ax^2 + bxy + cy^2$ hacia una forma reducida.

Denotemos por $a$ el menor entero positivo representado por $g$. En el Corolario 5.21 se vio cómo puede encontrarse $a$. Existen enteros $\alpha$ y $\beta$ tales que $A\alpha^2 + B\alpha\gamma + C\gamma^2 = a$. Nótese que $(\alpha, \gamma) = 1$; porque si $(\alpha, \gamma) = d$, entonces $F(\alpha/d, \gamma/d) = a/d^2$, lo cual implica $d = 1$ supuesto que $a$ fue número mínimo. Entonces, por el Teorema 1.3, existen los enteros $\beta$ y $\delta$ tales que $\alpha\delta - \beta\gamma = 1$ y se usan éstos para construir la transformación $x = \alpha u + \beta v, y = \gamma u + \delta v$ de determinante 1. Esta transformación lleva $g(x, y)$ hacia

$$\begin{aligned} h(u, v) &= A(\alpha u + \beta v)^2 + B(\alpha u + \beta v)(\gamma u + \delta v) + C(\gamma u + \delta v)^2 \\ &= au^2 + kuv + mv^2, \end{aligned}$$

digamos, donde $a$ es el entero definido anteriormente.

Ahora bien, para cualquier entero $j$ la transformación $u = x - jy$, $v = y$ tiene determinante 1 y lleva $h(u, v)$ hacia

$$f(x, y) = ax^2 + (k - 2aj)xy + (aj^2 - kj + m)y^2$$

Si se toma $j$ como el entero más próximo a $k/2a$, se tiene

$$-\frac{1}{2} \leqq \frac{k}{2a} - j \leqq \frac{1}{2}, -a \leqq k - 2aj \leqq a, \quad |k - 2aj| \leqq a$$

y puede escribirse

$$f(x, y) = ax^2 + bxy + cy^2, \quad |b| \leqq a.$$

Ahora bien $g \sim f$, $g$ es positivo y $f(0, 1) = c$. Por tanto, $g$ representa a $c$ y $c$ es positivo, de donde $c \geqq a$.

**Teorema 5.26** *Si dos formas reducidas son equivalentes, son idénticas.*

*Demostración.* Sean $ax^2 + bxy + cy^2$ y $Ax^2 + Bxy + Cy^2$ formas reducidas equivalentes. Puede suponerse que $a \geqq A$ y que (5.20) es la transformación que lleva una hacia la otra. Entonces los coeficientes satisfacen (5.22).

Primero se probará que $a = A$. Se tiene $0 \leqq b \leqq a \leqq c$ y usando la sencilla desigualdad $\alpha^2 + \gamma^2 \geqq 2|\alpha\gamma|$ se encuentra

(5.23) $$A = a\alpha^2 + b\alpha\gamma + c\gamma^2 \geqq a\alpha^2 + c\gamma^2 - b|\alpha\gamma|$$
$$\geqq a\alpha^2 + a\gamma^2 - b|\alpha\gamma| \geqq 2a|\alpha\gamma| - b|\alpha\gamma| \geqq a|\alpha\gamma|.$$

Supuesto que $a \geqq A > 0$ se deduce que $|\alpha\gamma| \leqq 1$. Si $|\alpha\gamma| = 0$ se tiene

(5.24) $$A = a\alpha^2 + c\gamma^2 \geqq a\alpha^2 + a\gamma^2 \geqq a$$

porque $\alpha$ y $\gamma$ no son ambos cero. Si $|\alpha\gamma| = 1$, entonces (5.23) se reduce inmediatamente al mismo resultado, $A \geqq a$. Así se tiene $A \geqq a$ en ambos casos y esto, con $a \geqq A$, implica que $a = A$.

Ahora que se tiene $a = A > 0$ sólo se necesita probar que $b = B$ o bien $c = C$, dado que uno se deduce del otro porque, por el Teorema 5.24, $b^2 - 4ac = B^2 - 4AC$. Así que el caso $c = C$ no requiere demostración adicional. Ya que $a = A$ pueden intercambiarse las formas, si fuera necesario, y puede suponerse $c > C$. Entonces se tiene $c > a$ ya que $C \geqq A = a$. Esto excluye la posibilidad $|\alpha\gamma| = 1$, porque si $|\alpha\gamma| = 1$ entonces $c\gamma^2 > a\gamma^2$ y (5.23) entonces implicaría $A > a|\alpha\gamma| = a$. Ahora que se tiene $|\alpha\gamma| = 0$ puede probarse que $\gamma = 0$, porque de otra manera se tendría otra vez $c\gamma^2 > a\gamma^2$ y (5.24) implicaría $A > a$.

Se han limitado las posibilidades hasta $a = A$, $a < c$, $\gamma = 0$. Dado que el determinante $\Delta = \alpha\delta - \beta\gamma$ es $\pm 1$, también se tiene $\alpha\delta = \pm 1$. Entonces, por (5.22), se tiene $B = 2a\alpha\beta \pm b$. Hay dos casos.

Primero, supóngase que $B = 2a\alpha\beta + b$. Entonces $0 \leqq b \leqq a$ y $0 \leqq B \leqq A = a$ implica que $-A \leqq B - b \leqq a$. Pero $B - b = 2a\ \alpha\beta$ es un múltiplo de $2a$ así que queda $B - b = 0$, $b = B$.

Segundo, supóngase que $B = 2a\alpha\beta - b$. En este caso se encuentra $0 \leqq B + b \leqq 2a$ y $B + b$ es un múltiplo de $2a$. Se tiene $B + b = 0$ o bien $B + b = 2a$. Ya que $0 \leqq b \leqq a$ y $0 \leqq B \leqq a$ se tiene $b = B = 0$ si $B + b = 0$ y $b = B = a$ si $B + b = 2a$. Nuevamente $b = B$.

Esto complementa la demostración puesto que, en todo caso, $a = A$, $b = B$, $c = C$.

Los dos últimos teoremas muestran que la Definición 5.2 es precisamente lo que se desea. Nos proporciona una y precisamente una representante para cada clase de equivalencias de formas cuadráticas binarias positivas. Debe observarse que la Definición 5.1 no es la única manera en la cual pueden ponerse las formas cuadráticas binarias positivas dentro de las clases de equivalencias. De hecho, algunos autores demandan que la transformación tenga determinante 1 en su definición de equivalencia. Entonces aplican una definición ligeramente diferente de forma reducida para que todavía se cumplan los Teoremas 5.25 y 5.26 bajo sus definiciones de equivalencia y de formas reducidas.

**Teorema 5.27** *Existe sólo un número finito de formas reducidas que tengan un discriminante dado.*

*Demostración.* Sea $-d$ cualquier entero negativo. Si $ax^2 + bxy + cy^2$ es una forma reducida con discriminante $-d$, entonces $b^2 - 4ac = -d$ y $0 \leqq b \leqq a \leqq c$. Así se tiene $d = 4ac - b^2 \geqq 4ac - ac \geqq 3a^2$ así como $0 \leqq b \leqq a$, de modo que hay cuando más $\sqrt{d/3}$ valores posibles para $a > 0$, y cuando más $a + 1$ valores para $b$ correspondientes a cada uno de $a$. Finalmente, hay cuando más un $c$ para cada $a$, $b$, tal que $4ac - b^2 = d$.

Encontremos todas las formas reducidas con $d \leqq 16$. Se tiene $1 \leqq a \leqq \sqrt{16/3}$, $a = 1$ o bien 2. Correspondiendo a $a = 1$, $b = 0$ se tiene $d = 4c$ y puede tomarse $c = 1, 2, 3$, o bien 4. Correspondiendo a $a = 1$, $b = 1$ se tiene $d = 4c - 1$ y otra vez puede tomarse $c = 1, 2, 3$ o bien 4. De modo semejante se encuentra $a = 2$, $b = 0$, $d = 8c$ y $a = 2$, $b = 1$, $d = 8c - 1$, $c = 2$ y $a = 2$, $b = 2$, $d = 8c - 4$, $c = 2$. Haciendo una lista de las formas reducidas de acuerdo con los valores de $d$ se obtiene la siguiente tabla.

$$d = 3,\ x^2 + xy + y^2$$
$$d = 4,\ x^2 + y^2$$
$$d = 7,\ x^2 + xy + 2y^2$$
$$d = 8,\ x^2 + 2y^2$$
$$d = 11,\ x^2 + xy + 3y^2$$
$$d = 12,\ x^2 + 3y^2,\ 2x^2 + 2xy + 2y^2$$
$$d = 15,\ x^2 + xy + 4y^2,\ 2x^2 + xy + 2y^2$$
$$d = 16,\ x^2 + 4y^2,\ 2x^2 + 2y^2.$$

Para $d = 3, 4, 7, 8, 11$, existe precisamente una forma reducida de discriminante $-d$. Para estos valores de $d$, cualquier forma positiva con discriminante $-d$ representará el mismo conjunto de enteros que el que representa la forma reducida correspondiente. Por ejemplo, el Corolario 5.14 determinó el conjunto de enteros representado por $x^2 + y^2$ y éste es el conjunto de enteros representado por cualquier forma positiva de discriminante $-4$.

El caso $d = 12$ es un poco diferente puesto que existen dos formas reducidas de discriminante $-12$. Pero en la primera forma $x^2 + 3y^2$ los coeficientes son relativamente primos mientras que en la segunda forma $2x^2 + 2xy + 2y^2$ los coeficientes son todos divisibles entre 2. De (5.22) es obvio que cualquier forma equivalente a $2x^2 + 2xy + 2y^2$ también tendrá todos sus coeficientes divisibles entre 2. También por (5.22), cualquier forma positiva con discriminante $-12$, con todos sus coeficientes divisibles entre 2, será equivalente a una forma reducida que tenga todos sus coeficientes divisibles entre 2, de aquí que sea equivalente

a $2x^2 + 2xy + 2y^2$. Por tanto, puede hacerse la afirmación: supóngase que $f$ es una forma positiva de discriminante $-12$. Si los coeficientes de $f$ son relativamente primos, entonces $f$ representa la misma clase que la que representa $x^2 + 3y^2$. Si los coeficientes no son relativamente primos, entonces $f$ representa la misma clase de la que representa $2x^2 + 2xy + 2y^2$. El caso $d = 16$ puede tratarse de manera semejante.

El caso $d = 15$ es todavía diferente y más complicado. Aquí se tienen dos formas reducidas y en ambas los coeficientes son relativamente primos. Existen dos formas para distinguir entre las formas equivalentes a una o a la otra forma reducida sin tener que producir realmente la forma reducida recorriendo los pasos de la demostración del Teorema 5.25. No obstante, no lo consideraremos.

Hasta aquí llevaremos el tópico de las formas cuadráticas. Hay algo más que puede hacerse. Por una parte, no se ha discutido la cuestión de cómo determinar la clase de enteros representada por una forma reducida. Los métodos aplicados para obtener el Corolario 5.14 pueden extenderse para obtener alguna información. Un estudio adicional de la transformación presentada en esta sección también es muy útil.

**Problemas**

1. Probar que las siguientes formas son equivalentes:
   $ax^2 + bxy + cy^2$, $cx^2 + bxy + ay^2$, $ax^2 - bxy + cy^2$, $cx^2 - bxy + ay^2$.
2. Encontrar la forma reducida equivalente a
   *a*) $3x^2 + 7xy + 5y^2$;
   *b*) $2x^2 - 5xy + 4y^2$;
   *c*) $2x^2 + xy + 6y^2$;
   *d*) $3x^2 + xy + y^2$.
3. Probar que no hay formas cuadráticas binarias con discriminante congruente a 2 o bien 3 módulo 4.
4. Encontrar la forma reducida equivalente a $7x^2 + 25xy + 23y^2$.
5. Probar que a cualquier forma cuadrática binaria positiva dada le corresponde un número infinito de formas equivalentes.
6. Probar que hay solamente una forma reducida de discriminante $-43$. De aquí probar que dos formas cuadráticas binarias positivas cualesquiera de discriminante $-43$ son equivalentes.
7. Probar que dos formas cuadráticas binarias positivas cualesquiera de discriminante $-67$ son equivalentes.
8. Denotar la forma positiva $ax^2 + bxy + cy^2$ por $[a, b, c]$. Probar que, como una variación del método del Teorema 5.25, la forma reducida equivalente a $[a, b, c]$ puede obtenerse mediante una sucesión finita de operaciones de tres tipos:
   1. en el caso de $a > c$, reemplazando $[a, b, c]$ por $[c, b, a]$;
   2. en el caso de $|b| > a$, reemplazando $[a, b, c]$ por $[a, b - 2aj, c_1]$, donde se escoge $j$ de manera que $|b - 2aj| \leqq a$ y $c_1$ está determinado por la igualdad de los discriminantes, $b^2 - 4ac = (b - 2aj)^2 - 4ac_1$;
   3. en el caso de $b < 0$, reemplazando $[a, b, c]$ por $[a, -b, c]$.

*Capítulo 6*

# *Fracciones de Farey*

## 6.1 Sucesiones de Farey

Construyamos una tabla en la siguiente forma. En el primer renglón escribimos $0/1$ y $1/1$. Para $n = 2, 3, \cdots$ aplicamos la regla: Formar el $n$-ésimo renglón copiando el $(n - 1)$-ésimo en orden pero insertando la fracción $(a + a')/(b + b')$ entre las fracciones consecutivas $a/b$ y $a'/b'$ del $(n - 1)$-ésimo renglón si $b + b' \leqq n$. Así, dado que $1 + 1 \leqq 2$ se inserta $(0 + 1)/(1 + 1)$ entre $0/1$ y $1/1$ y se obtiene $0/1$, $1/2$, $1/1$, para el segundo renglón. El tercer renglón es $0/1$, $1/3$, $1/2$, $2/3$, $1/1$. Para obtener el cuarto renglón se insertan $(0+1)/(1+3)$ y $(2+1)/(3+1)$ pero no $(1 + 1)/(3 + 2)$ y $(1 + 2)/(2 + 3)$. Los primeros cinco renglones de la tabla son

$$\begin{array}{ccccccccccc}
\frac{0}{1} & & & & & & & & & & \frac{1}{1} \\
\frac{0}{1} & & & & & \frac{1}{2} & & & & & \frac{1}{1} \\
\frac{0}{1} & & & \frac{1}{3} & & \frac{1}{2} & & \frac{2}{3} & & & \frac{1}{1} \\
\frac{0}{1} & & \frac{1}{4} & \frac{1}{3} & & \frac{1}{2} & & \frac{2}{3} & \frac{3}{4} & & \frac{1}{1} \\
\frac{0}{1} & \frac{1}{5} & \frac{1}{4} & \frac{1}{3} & \frac{2}{5} & \frac{1}{2} & \frac{3}{5} & \frac{2}{3} & \frac{3}{4} & \frac{4}{5} & \frac{1}{1}
\end{array}$$

Hasta este renglón, por lo menos, la tabla tiene un número de propiedades interesantes. Todas las fracciones que aparecen están en forma

reducida; todas las fracciones reducidas $a/b$ tales que $0 \leqq a/b \leqq 1$ y $b \leqq n$ aparecen en el $n$-ésimo renglón; si $a/b$ y $a'/b'$ son fracciones consecutivas en el $n$-ésimo renglón, entonces $a'b - ab' = 1$ y $b + b' > n$. Se probarán todas estas propiedades para la tabla completa.

**Teorema 6.1** *Si $a/b$ y $a'/b'$ son fracciones consecutivas en el $n$-ésimo renglón, digamos con $a/b$ a la izquierda de $a'/b'$, entonces $a'b - ab' = 1$.*

*Demostración.* Esto es cierto para $n = 1$. Supóngase que es verdad para el $(n - 1)$-ésimo renglón. Cualesquiera fracciones consecutivas en el $n$-ésimo renglón serán $a/b$, $a'/b'$ o bien $a/b$, $(a + a')/(b + b')$ o bien $(a + a')/(b + b')$, $a'/b'$ donde $a/b$ y $a'/b'$ son fracciones consecutivas en el $(n - 1)$-ésimo renglón. Pero entonces se tiene $a'b - ab' = 1$, $(a + a')b - a(b + b') = a'b - ab' = 1$, $a'(b + b') - (a + a')b' = a'b - ab' = 1$ y el teorema se demuestra por inducción matemática.

**Corolario 6.2** *Toda $a/b$ en la tabla está en forma reducida, esto es,* $(a, b) = 1$.

**Corolario 6.3** *Las fracciones en cada renglón están enlistadas en orden de magnitud.*

**Teorema 6.4** *Si $a/b$ y $a'/b'$ son fracciones consecutivas en cualquier renglón, entonces entre todas las fracciones racionales con valores entre estos dos, $(a + a')/(b + b')$ es la fracción única con el menor denominador.*

*Demostración.* En primer lugar, la fracción $(a + a')/(b + b')$ será la primera fracción que se inserte entre $a/b$ y $a'/b'$ conforme se continúe avanzando en los renglones de la tabla. Primero aparecerá en el $(b + b')$-ésimo renglón. Por tanto, se tiene

$$\frac{a}{b} < \frac{a + a'}{b + b'} < \frac{a'}{b'}$$

por el Corolario 6.3

Ahora considérese cualquier fracción $x/y$ entre $a/b$ y $a'/b'$ de modo que $a/b < x/y < a'/b'$. Entonces

$$(6.1)\qquad \frac{a'}{b'} - \frac{a}{b} = \left(\frac{a'}{b'} - \frac{x}{y}\right) + \left(\frac{x}{y} - \frac{a}{b}\right)$$
$$= \frac{a'y - b'x}{b'y} + \frac{bx - ay}{by} \geqq \frac{1}{b'y} + \frac{1}{by} = \frac{b + b'}{bb'y},$$

y por lo tanto

$$\frac{b + b'}{bb'y} \leqq \frac{a'b - ab'}{bb'} = \frac{1}{bb'},$$

lo cual implica $y \geqq b + b'$. Si $y > b + b'$ entonces $x/y$ no tiene el menor denominador entre las fracciones comprendidas entre $a/b$ y $a'/b'$. Si $y = b + b'$, entonces la desigualdad en (6.1) debe volverse igualdad y se tiene $a'y - b'x = 1$ y $bx - ay = 1$. Resolviendo se encuentra $x = a + a'$, $y = b + b'$ y de aquí que $(a + a')/(b + b')$ es la única fraccionaria racional que se encuentra entre $a/b$ y $a'/b'$.

**Teorema 6.5** Si $0 \leqq x \leqq y$, $(x, y) = 1$, *entonces la fracción* $x/y$ *aparece en el* $y$-ésimo *y en todos los últimos renglones.*

*Demostración.* Esto es obvio si $y = 1$. Supóngase que es cierto para $y = y_0 - 1$, con $y_0 > 1$. Entonces si $y = y_0$, la fracción $x/y$ no puede estar en el $(y - 1)$-ésimo renglón, por definición, y por tanto debe estar, en valor, entre dos fracciones consecutivas $a/b$ y $a'/b'$ del $(y - 1)$-ésimo renglón. Así que $a/b < x/y < a'/b'$. Supuesto que

$$\frac{a}{b} < \frac{a + a'}{b + b'} < \frac{a'}{b'}$$

y $a/b$, $a'/b'$ son consecutivas, la fracción $(a + a')/(b + b')$ no está en el $(y - 1)$-ésimo renglón y de aquí que $b + b' > y - 1$, por nuestra hipótesis de inducción. Pero, por el Teorema 6.4, $y \geqq b + b'$ y así se tiene $y = b + b'$. Entonces la parte de unicidad del Teorema 6.4 establece que $x = a + a'$. De donde $x/y = (a + a')/(b + b')$ entra en el $y$-ésimo renglón y entonces está en todos los últimos renglones.

**Corolario 6.6** *El* $n$-ésimo *renglón consiste de todas las fracciones racionales reducidas* $a/b$ *tales que* $0 \leqq a/b \leqq 1$ *y* $0 < b \leqq n$. *Las fracciones se enlistan en el orden de su magnitud.*

**Definición 6.1** *La sucesión de todas las fracciones reducidas con denominadores que no excedan a* $n$, *enlistadas en orden de su magnitud, recibe el nombre de sucesión de Farey de orden* $n$.

El $n$-ésimo renglón de nuestra tabla da esa parte de la sucesión de Farey de orden $n$ que se encuentra entre 0 y 1 y, por tanto, la sucesión de Farey completa de orden $n$ puede obtenerse a partir del $n$-ésimo renglón, sumando y sustrayendo los enteros. Por ejemplo, la sucesión de Farey de orden 2 es

$$\ldots, \frac{-3}{1}, \frac{-5}{2}, \frac{-2}{1}, \frac{-3}{2}, \frac{-1}{1}, \frac{-1}{2}, \frac{0}{1}, \frac{1}{2}, \frac{1}{1}, \frac{3}{2}, \frac{2}{1}, \frac{5}{2}, \frac{3}{1}, \ldots.$$

Esta definición de las sucesiones de Farey parece ser la más conveniente. No obstante, algunos autores prefieren restringir las fracciones al intervalo de 0 a 1; definen las sucesiones de Farey precisamente como los renglones de nuestra tabla.

Cualquier fracción reducida con denominador positivo $\leqq n$ es un miembro de la sucesión de Farey de orden $n$ y puede llamarse fracción de Farey de orden $n$. Nótese que las fracciones consecutivas $a/b$ y $a'/b'$ en la sucesión de Farey de orden $n$ satisface la igualdad del Teorema 6.1 y también la desigualdad $b + d > n$.

**Problemas**

1. Sean $a/b$ y $a'/b'$ las fracciones inmediatamente a la izquierda y a la derecha de la fracción $\frac{1}{2}$ en la sucesión de Farey de orden $n$. Probar que $b = b' = 1 + 2[(n - 1)/2]$, esto es $b$ es el máximo entero impar $\leqq n$. También probar que $a + a' = b$.
2. Probar que el número de fracciones de Farey $a/b$ de orden $n$ que satisfacen las desigualdades $0 \leqq a/b \leqq 1$ es $1 + \sum_{j=1}^{n} \phi(j)$ y que su suma es exactamente la mitad de este valor.
3. Sean $a/b$, $a'/b'$, $a''/b''$ tres fracciones consecutivas cualesquiera en la sucesión de Farey de orden $n$. Probar que $a'/b' = (a + a'')/(b + b'')$.
4. Supóngase que $a/b$ y $a'/b'$ recorren todos los pares de fracciones adyacentes en la sucesión de Farey de orden $n > 1$. Probar que
$$\text{mín}\left(\frac{a'}{b'} - \frac{a}{b}\right) = \frac{1}{n(n-1)} \text{ y } \text{máx}\left(\frac{a'}{b'} - \frac{a}{b}\right) = \frac{1}{n}.$$
5. Considérese dos números racionales $a/b$ y $c/d$ tales que $ad - bc = 1$, $b > 0$, $d > 0$. Definir $n$ como máx $(b, d)$ y probar que $a/b$ y $c/d$ son fracciones adyacentes en la sucesión de Farey de orden $n$.
6. Probar que las dos fraciones descritas en el problema anterior no son necesariamente adyacentes en la sucesión de Farey de orden $n + 1$.
7. Considérense las fracciones de $0/1$ a $1/1$ inclusive en la sucesión de Farey de orden $n$. Leyendo de izquierda a derecha, sean los denominadores de estas fracciones $a_1, a_2, \cdots, a_k$ de modo que $a_1 = 1$ y $a_k = 1$. Probar que $\sum_{j=1}^{n-1} (a_j a_{j+1})^{-1} = 1$.

## 6.2 Aproximaciones racionales

**Teorema 6.7** *Si $a/b$ y $c/d$ son fracciones de Farey de orden $n$ tales que ninguna otra fracción de Farey de orden $n$ se encuentra entre ellas, entonces*
$$\left|\frac{a}{b} - \frac{a+c}{b+d}\right| = \frac{1}{b(b+d)} \leqq \frac{1}{b(n+1)},$$
*y*
$$\left|\frac{c}{d} - \frac{a+c}{b+d}\right| = \frac{1}{d(b+d)} \leqq \frac{1}{d(n+1)}.$$

*Demostración.* Se tiene
$$\left|\frac{a}{b} - \frac{a+c}{b+d}\right| = \frac{|ad - bc|}{b(b+d)} = \frac{1}{b(b+d)} \leqq \frac{1}{b(n+1)}$$

por el Teorema 6.1 y el hecho de que $b + d \geqq n + 1$. La segunda fórmula se demuestra de manera semejante.

**Teorema 6.8** *Si $n$ es un entero positivo y $x$ es real, existe un número racional $a/b$ tal que $0 < b \leqq n$ y*

$$\left| x - \frac{a}{b} \right| \leqq \frac{1}{b(n+1)}.$$

*Demostración.* Considérese el conjunto de todas las fracciones de Farey de orden $n$ y todas las fracciones $(a + c)/(b + d)$ como se describieron en el Teorema 6.7. Para algunas fracciones $a/b$ y $c/d$, el número $x$ se encontrará en el intervalo cerrado entre $a/b$ y $(a + c)/(b + d)$. Entonces, por el Teorema 6.7,

$$\left| x - \frac{a}{b} \right| \leqq \left| \frac{a}{b} - \frac{a+c}{b+d} \right| \leqq \frac{1}{b(n+1)}.$$

**Teorema 6.9** *Si $\xi$ es real e irracional, existe un número infinito de números racionales $a/b$ tales que*

$$\left| \xi - \frac{a}{b} \right| < \frac{1}{b^2}.$$

*Demostración.* Para cada $n = 1, 2, \cdots$, con base en el Teorema 6.8, pueden encontrarse un $a_n$ y un $b_n$ tales que $0 < b_n \leqq n$ y

$$\left| \xi - \frac{a_n}{b_n} \right| \leqq \frac{1}{b_n(n+1)} < \frac{1}{b_n^2}.$$

Muchos de los $b_n$ pueden ser iguales entre sí, pero habrá un número infinito de distintos. Porque si no hubiera un número infinito de distintos, solamente habría un número finito de valores distintos tomados por $|\xi - a_n/b_n|$, $n = 1, 2, 3, \cdots$. Entonces habría entre estos valores un menor y sería el valor de $|\xi - a_n/b_n|$ para algún $n$, digamos $n = k$. Se tendría $|\xi - a_n/b_n| \geqq |\xi - a_k/b_k|$ para todo $n = 1, 2, 3, \cdots$. Pero $|\xi - a_k/b_k| > 0$ dado que $\xi$ es irracional y puede encontrarse un $n$ lo suficientemente grande para que

$$\frac{1}{n+1} < \left| \xi - \frac{a_k}{b_k} \right|.$$

Esto conduce a una contradicción dado que ahora se tendría

$$\left| \xi - \frac{a_k}{b_k} \right| \leqq \left| \xi - \frac{a_n}{b_n} \right| \leqq \frac{1}{b_n(n+1)} \leqq \frac{1}{n+1} < \left| \xi - \frac{a_k}{b_k} \right|.$$

La condición de que $\xi$ es irracional es necesaria en el teorema. Porque si $x$ es cualquier número racional puede escribirse $x = r/s$, $s > 0$. Entonces, si $a/b$ es cualquier fracción tal que $a/b \neq r/s$, $b > s$, se tiene

$$\left|\frac{r}{s} - \frac{a}{b}\right| = \frac{|rb - as|}{sb} \geqq \frac{1}{sb} > \frac{1}{b^2}.$$

De aquí que todas las fracciones $a/b$, $b > 0$, que satisfacen $|x - a/b| < 1/b^2$ tienen denominadores $b \leqq s$ y sólo puede haber un número finito de tales fracciones.

El resultado del Teorema 6.9 puede mejorarse, tal y como se demostrará en el Teorema 6.11. En la Sección 7.6 se darán demostraciones diferentes de los Teoremas 6.11 y 6.12.

**Lema 6.10** *Si $x$ y $y$ son enteros positivos entonces no pueden cumplirse simultáneamente las dos desigualdades*

$$\frac{1}{xy} \geqq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2} + \frac{1}{y^2}\right) \text{ y } \frac{1}{x(x+y)} \geqq \frac{1}{\sqrt{5}}\left(\frac{1}{x^2} + \frac{1}{(x+y)^2}\right)$$

*Demostración.* Las dos desigualdades pueden escribirse como

$$\sqrt{5}\, xy \geqq y^2 + x^2, \qquad \sqrt{5}x(x+y) \geqq (x+y)^2 + x^2.$$

Sumando estas desigualdades se obtiene $\sqrt{5}(x^2 + 2xy) \geqq 3x^2 + 2xy + 2y^2$, de aquí que $2y^2 - 2(\sqrt{5} - 1)xy + (3 - \sqrt{5})x^2 \leqq 0$. Multiplicando esto por 2 se lleva a la forma $4y^2 - 4(\sqrt{5} - 1)xy + (5 - 2\sqrt{5} + 1)x^2 \leqq 0$, $(2y - (\sqrt{5} - 1)x)^2 \leqq 0$. Esto es imposible para los enteros positivos $x$ y $y$ debido a que $\sqrt{5}$ es irracional.

**Teorema 6.11** (*Hurwitz*) *Dado cualquier número irracional $\xi$, existe un número infinito de números racionales diferentes $h/k$ tales que*

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{\sqrt{5}\, k^2} \tag{6.2}$$

*Demostración.* Sea $n$ un entero positivo. Existen dos fracciones consecutivas $a/b$ y $c/d$ en la sucesión de Farey de orden $n$, tales que $a/b < \xi < c/d$. Ya sea que $\xi < (a + c)/(b + d)$ o bien $\xi > (a + c)/(b + d)$.

*Caso I.* $\xi < (a + c)/(b + d)$. Supóngase que

$$\xi - \frac{a}{b} \geqq \frac{1}{b^2\sqrt{5}}, \quad \frac{a+c}{b+d} - \xi \geqq \frac{1}{(b+d)^2\sqrt{5}}, \quad \frac{c}{d} - \xi \geqq \frac{1}{d^2\sqrt{5}}.$$

Sumando las desigualdades se obtiene

$$\frac{c}{d} - \frac{a}{b} \geqq \frac{1}{d^2\sqrt{5}} + \frac{1}{b^2\sqrt{5}}, \quad \frac{a+c}{b+d} - \frac{a}{b} \geqq \frac{1}{(b+d)^2\sqrt{5}} + \frac{1}{b^2\sqrt{5}},$$

de aquí que

$$\frac{1}{bd} = \frac{cb - ad}{bd} = \frac{c}{d} - \frac{a}{b} \geqq \frac{1}{\sqrt{5}}\left(\frac{1}{b^2} + \frac{1}{d^2}\right)$$

y

$$\frac{1}{b(b+d)} = \frac{(a+c)b - (b+d)a}{b(b+d)} \geqq \frac{1}{\sqrt{5}}\left(\frac{1}{b^2} + \frac{1}{(b+d)^2}\right)$$

Estas dos desigualdades contradicen el Lema 6.10. Por lo tanto, en este caso, por lo menos una de $a/b$, $c/d$, $(a + c)/(b + d)$ servirá como $h/k$.

*Caso II.* $\xi > (a + c)/(b + d)$. Supóngase que

$$\xi - \frac{a}{b} \geqq \frac{1}{b^2\sqrt{5}}, \quad \xi - \frac{a+c}{b+d} \geqq \frac{1}{(b+d)^2\sqrt{5}}, \quad \frac{c}{d} - \xi \geqq \frac{1}{d^2\sqrt{5}}.$$

Sumando como antes, se obtiene

$$\frac{c}{d} - \frac{a}{b} \geqq \frac{1}{d^2\sqrt{5}} + \frac{1}{b^2\sqrt{5}}, \qquad \frac{c}{d} - \frac{a+c}{b+d} \geqq \frac{1}{d^2\sqrt{5}} + \frac{1}{(b+d)^2\sqrt{5}},$$

y de aquí que

$$\frac{1}{bd} \geqq \frac{1}{\sqrt{5}}\left(\frac{1}{d^2} + \frac{1}{b^2}\right), \qquad \frac{1}{d(b+d)} \geqq \frac{1}{\sqrt{5}}\left(\frac{1}{(b+d)^2} + \frac{1}{d^2}\right),$$

lo cual también contradice el Lema 6.10. Nuevamente, por lo menos una de $a/b$, $c/d$, $(a + c)/(b + d)$ servirá como $h/k$.

Se ha demostrado la existencia de alguna $h/k$ que satisface (6.2). Esta $h/k$ depende de la selección de $n$. De hecho $h/k$ es $a/b$, $c/d$ o bien $(a + c)/(b + d)$, donde $a/b$ y $c/d$ son fracciones consecutivas en la sucesión de Farey de orden $n$ y $a/b < \xi < c/d$. Aplicando el Teorema 6.7 se ve que

$$\left|\xi - \frac{h}{k}\right| \leqq \frac{1}{b(n+1)} \quad \text{ó} \quad \left|\xi - \frac{h}{k}\right| \leqq \frac{1}{d(n+1)}.$$

En cada caso se tiene

$$\left|\xi - \frac{h}{k}\right| \leqq \frac{1}{n+1}.$$

Se desea establecer que existe un número infinito de $h/k$ que satisfacen (6.2). Supóngase que se tiene cualquier $h_1/k_1$ que satisface (6.2). Entonces $\left|\xi - \frac{h_1}{k_1}\right|$ es positivo y puede escogerse $n > 1 \Big/ \left|\xi - \frac{h_1}{k_1}\right|$. La sucesión de Farey de orden $n$ entonces proporciona un $h/k$ que satisface (6.2) y tal que

$$\left|\xi - \frac{h}{k}\right| \leqq \frac{1}{n+1} < \left|\xi - \frac{h_1}{k_1}\right|.$$

Esto demuestra que existe un número infinito de números racionales $h/k$ que satisfacen (6.2) ya que, dado cualquier número racional, puede encontrarse otro que sea más próximo a $\xi$.

**Teorema 6.12** *La constante* $\sqrt{5}$ *del Teorema* 6.11 *es la mejor posible. En otras palabras, el Teorema* 6.11 *no se cumple si* $\sqrt{5}$ *se reemplaza por cualquier valor mayor.*

*Demostración.* Sólo se necesita presentar un $\xi$ para el cual $\sqrt{5}$ no pueda reemplazarse por un valor mayor. Tomemos $\xi = \frac{1}{2}(1 + \sqrt{5})$. Entonces

$$(x - \xi)\left(x - \frac{1 - \sqrt{5}}{2}\right) = x^2 - x - 1.$$

Entonces, para los enteros $h$, $k$ con $k > 0$, se tiene

$$(6.3) \quad \left|\frac{h}{k} - \xi\right|\left|\frac{h}{k} - \xi + \sqrt{5}\right| = \left|\left(\frac{h}{k} - \xi\right)\left(\frac{h}{k} - \frac{1 - \sqrt{5}}{2}\right)\right|$$
$$= \left|\frac{h^2}{k^2} - \frac{h}{k} - 1\right| = \frac{1}{k^2}\,|h^2 - hk - k^2|.$$

La expresión de la izquierda en (6.3) no es cero debido a que tanto $\xi$ como $\sqrt{5} - \xi$ son irracionales. La expresión $|h^2 - hk - k^2|$ es un entero no negativo. Por tanto $|h^2 - hk - k^2| \geqq 1$ y se tiene

$$(6.4) \quad \left|\frac{h}{k} - \xi\right|\left|\frac{h}{k} - \xi + \sqrt{5}\right| \geqq \frac{1}{k^2}.$$

Ahora supóngase que se tiene una sucesión infinita de números racionales $h_j/k_j$, $k_j > 0$ y un número real positivo $m$ tal que

$$(6.5) \quad \left|\frac{h_j}{k_j} - \xi\right| < \frac{1}{mk_j^2}.$$

Entonces $k_j\xi - \dfrac{1}{mk_j} < h_j < k_j\xi + \dfrac{1}{mk_j}$, y esto implica que hay solamente un número finito de $h_j$ correspondientes a cada valor de $k_j$. Por lo tanto, se tiene $k_j \to \infty$ conforme $j \to \infty$. También, por (6.4), (6.5) y la desigualdad del triángulo se tiene

$$\frac{1}{k_j^2} \leqq \left|\frac{h_j}{k_j} - \xi\right|\left|\frac{h_j}{k_j} - \xi + \sqrt{5}\right| < \frac{1}{mk_j^2}\left(\frac{1}{mk_j^2} + \sqrt{5}\right),$$

de aquí que

$$m < \frac{1}{mk_j^2} + \sqrt{5},$$

y de donde

$$m \leqq \lim_{j\to\infty} \left(\frac{1}{mk_j^2} + \sqrt{5}\right) = \sqrt{5}.$$

**Problemas**

1. Probar que para cada número real $x$ existe un número infinito de pares de enteros $a$, $b$ con $b$ positivo tal que $|bx - a| < (\sqrt{5}\, b)^{-1}$.
2. Sea $\xi$ un irracional. Sean $\lambda > 0$ y $\alpha > 2$ números reales. Probar que existe sólo un número finito de racionales $h/k$ que satisfacen
$$\left| \xi - \frac{h}{k} \right| < \frac{1}{\lambda k^{\alpha}}.$$
3. Supóngase que $h = a$, $k = b$ es una solución de la desigualdad (6.2) para algún irracional $\xi$. Probar que sólo un número finito de pares $h$, $k$ en el conjunto $\{h = ma,\ k = mb;\ m = 1, 2, 3, \cdots\}$ satisfacen (6.2).
4. Sea $\alpha > 1$ un número real. Supóngase que para algún número real $\beta$ existe un número infinito de números racionales $h/k$ tales que $|\beta - h/k| < k^{-\alpha}$. Probar que $\beta$ es irracional.
5. Probar que los siguientes números son irracionales:
$$\sum_{j=1}^{\infty} 2^{-3^j}, \qquad \sum_{j=1}^{\infty} 2^{-j!}.$$

# Capítulo 7

# Fracciones continuadas simples

## 7.1 El algoritmo euclidiano

Dada cualquier fracción racional $u_0/u_1$, en su más simple expresión de manera que $(u_0, u_1) = 1$ y $u_1 > 0$, aplicamos el algoritmo euclidiano tal y como se formuló en el Teorema 1.11 para obtener

$$
\begin{aligned}
(7.1) \qquad u_0 &= u_1 a_0 + u_2, & 0 < u_2 < u_1 \\
u_1 &= u_2 a_1 + u_3, & 0 < u_3 < u_2 \\
u_2 &= u_3 a_2 + u_4, & 0 < u_4 < u_3 \\
u_{j-1} &= u_j a_{j-1} + u_{j+1}, & 0 < u_{j+1} < u_j \\
u_j &= u_{j+1} a_j.
\end{aligned}
$$

La notación se ha alterado respecto a la dada en el Teorema 1.11, reemplazando $b,\ c$ por $u_0, u_1, r_1, r_2, \cdots, r_j$ por $u_2, u_3, \cdots, u_{j+1}$ y $q_1, q_2, \cdots, q_{j+1}$ por $a_0, a_1, \cdots, a_j$. La forma (7.1) es un poco más apropiada para nuestros propósitos actuales. Si escribimos $\xi_i$ en lugar de $u_i/u_{i+1}$ para todos los valores de $i$ en el rango $0 \leqq i \leqq j$, entonces las ecuaciones (7.1) se transforman en

$$(7.2) \qquad \xi_i = a_i + \frac{1}{\xi_{i+1}}, \quad 0 \leqq i \leqq j - 1; \quad \xi_j = a_j.$$

Si se toman las dos primeras de estas ecuaciones, aquellas para las cuales $i = 0$ e $i = 1$, y se elimina $\xi_1$, se obtiene

$$\xi_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\xi_2}}.$$

En este resultado se reemplaza $\xi_2$ por su valor dado en (7.2) y se continúa reemplazando $\xi_3, \xi_4, \cdots$, para obtener

$$\frac{u_0}{u_1} = \xi_0 = a_0 + \cfrac{1}{a_1 + \cfrac{\cdot}{\cdot \; \cdot \; + \cfrac{1}{a_{j-1} + \cfrac{1}{a_j}}}}. \tag{7.3}$$

Este es un desarrollo fraccionario continuado de $\xi_0$ o bien de $u_0/u_1$. Los enteros $a_i$ se llaman cocientes parciales dado que son los cocientes en la aplicación repetida del algoritmo de la división en las ecuaciones (7.1). Se supuso que la fracción racional $u_0/u_1$ tenía denominador positivo $u_1$, pero no puede hacerse una suposición semejante respecto a $u_0$. De aquí que $a_0$ puede ser positivo, negativo o bien cero. No obstante, supuesto que $0 < u_2 < u_1$, se nota que el cociente $a_1$ es positivo y, de modo semejante, los cocientes subsecuentes $a_2, a_3, \cdots, \cdots, a_j$ son enteros positivos. En el caso de que $j \geqq 1$, esto es si el conjunto (7.1) contiene más de una ecuación, entonces $a_j = u_j/u_{j+1}$ y $0 < u_{j+1} < u_j$ implica que $a_j > 1$.

Usaremos la notación $\langle a_0, a_1, \cdots, a_j \rangle$ para designar la fracción continuada en (7.3). En general, si $x_0, x_1, \cdots; x_j$ son números reales cualesquiera, todos positivos excepto tal vez $x_0$, se escribirá

$$\langle x_0, x_1, \cdots, x_j \rangle = x_0 + \cfrac{1}{x_1 + \cfrac{\cdot}{\cdot \; \cdot \; + \cfrac{1}{x_{j-1} + \cfrac{1}{x_j}}}}.$$

Se dice que tal fracción continuada finita es simple si todos los $x_i$ son enteros. Con frecuencia son útiles las siguientes fórmulas obvias:

$$\langle x_0, x_1, \cdots, x_j \rangle = x_0 + \frac{1}{\langle x_1, \cdots, x_j \rangle}$$
$$= \left\langle x_0, x_1, \cdots, x_{j-2}, x_{j-1} + \frac{1}{x_j} \right\rangle.$$

El símbolo $[x_0, x_1, \cdots, x_j]$ se usa frecuentemente para representar una fracción continuada. Nosotros usaremos la notación $\langle x_0, x_1, \cdots, x_j \rangle$ para evitar confusiones con el mínimo común múltiplo y el máximo entero.

**Problemas**

1. Desarrollar las fracciones racionales 17/3, 3/17 y 8/1 en fracciones continuadas simples finitas.
2. Probar que el conjunto (7.1) consiste de exactamente una ecuación si, y solamente si, $u_1 = 1$. ¿Bajo qué circunstancias $a_0 = 0$?
3. Convertir a números racionales: $\langle 2, 1, 4\rangle$; $\langle -3, 2, 12\rangle$; $\langle 0, 1, 1, 100\rangle$.
4. Dados los enteros positivos $b$, $c$, $d$ con $c > d$, probar que $\langle a, c\rangle < \langle a, d\rangle$ pero $\langle a, b, c\rangle > \langle a, b, d\rangle$ para cualquier entero $a$.
5. Sean $a_1, a_2 \cdots, a_n$ y $c$ números reales positivos. Probar que

$$\langle a_0, a_1, \cdots, a_n\rangle > \langle a_0, a_1, \cdots, a_n + c\rangle$$

se cumple si $n$ es impar, pero es falso si $n$ es par.

## 7.2 Unicidad

En la última sección se vio que una fracción como 51/22 puede desarrollarse en una fracción continuada simple, $51/22 = \langle 2, 3, 7\rangle$. Puede verificarse que 51/22 también puede expresarse como $\langle 2, 3, 6, 1\rangle$, pero resulta que éstas son las únicas dos representaciones de 51/22. En general, se observa que el desarrollo fraccionario continuado simple (7.3) tiene una forma alternativa

$$(7.4)\qquad \frac{u_0}{u_1} = \langle a_0, a_1, \cdots, a_{j-1}, a_j\rangle = \langle a_0, a_1, \cdots, a_{j-1}, a_j - 1, 1\rangle.$$

El resultado siguiente establece que éstos son los únicos dos desarrollos fraccionarios continuados simples de un número racional fijo.

**Teorema 7.1** *Si $\langle a_0, a_1, \cdots, a_j\rangle = \langle b_0, b_1, \cdots, b_n\rangle$ donde estas fracciones continuadas finitas son simples, y si $a_j > 1$ y $b_n > 1$ entonces $j = n$ y $a_i = b_i$ para $i = 0, 1, \cdots, n$.*

*Demostración.* Escribamos $y_i$ para la fracción continuada $\langle b_i, b_{i+1}, \cdots, b_n\rangle$ y observemos que

$$(7.5)\qquad y_i = \langle b_i, b_{i+1} \cdots, b_n\rangle = b_i + \frac{1}{\langle b_{i+1}, b_{i+2}, \cdots, b_n\rangle} = b_i + \frac{1}{y_{i+1}}.$$

Así se tiene $y_i > b_i$ y $y_i > 1$ para $i = 1, 2, \cdots, n-1$ y $y_n = b_n > 1$. En consecuencia; $b_i = [y_i]$ para todos los valores de $i$ en el rango $0 \leqq i \leqq n$. La hipótesis de que las fracciones continuadas son iguales pueden

escribirse en la forma $y_0 = \xi_0$, donde se ha aplicado la notación de la ecuación (7.3). Ahora bien, la definición de $\xi_i$ como $u_i/u_{i+1}$ implica que $\xi_{i+1} > 1$ para todos los valores de $i \geqq 0$, y así $a_i = [\xi_i]$ para $0 \leqq i \leqq j$, por las ecuaciones (7.2). A partir de que $y_0 = \xi_0$ se deduce que, tomando las partes enteras, $b_0 = [y_0] = [\xi_0] = a_0$. Por las ecuaciones (7.2) y (7.5) se obtiene

$$\frac{1}{\xi_1} = \xi_0 - a_0 = y_0 - b_0 = \frac{1}{y_1}, \quad \xi_1 = y_1, \quad a_1 = [\xi_1] = [y_1] = b_1.$$

Esto nos proporciona el principio de una demostración por inducción matemática. Ahora se establece que $\xi_i = y_i$ y $a_i = b_i$ implican que $\xi_{i+1} = y_{i+1}$ y $a_{i+1} = b_{i+1}$. Para ver esto, se usan otra vez las ecuaciones (7.2) y (7.5) para escribir

$$\frac{1}{\xi_{i+1}} = \xi_i - a_i = y_i - b_i = \frac{1}{y_{i+1}}, \quad \xi_{i+1} = y_{i+1}, \quad a_{i+1} = [\xi_{i+1}]$$
$$= [y_{i+1}] = b_{i+1}.$$

También debe concluirse que las fracciones continuadas tienen la misma longitud, esto es, que $j = n$. Porque supongamos, por ejemplo, que $j < n$. Con base en el argumento anterior se tiene $\xi_j = y_j$, $a_j = b_j$. Pero por (7.2), $\xi_j = a_j$ y, por (7.5), $y_j > b_j$, y así se llega a una contradicción. Si se hubiera supuesto que $j > n$, se hubiera llegado a una contradicción simétrica y, por lo tanto, $j$ debe ser igual a $n$ y queda demostrado el teorema.

**Teorema 7.2** *Cualquier fracción continuada simple finita representa un número racional. Inversamente, cualquier número racional puede expresarse como una fracción continuada simple finita y exactamente de dos maneras.*

*Demostración.* La primera observación puede establecerse mediante inducción matemática sobre el número de términos en la fracción continuada, por el uso de la fórmula

$$\langle a_0, a_1, \cdots, a_j \rangle = a_0 + \frac{1}{\langle a_1, a_2, \cdots, a_j \rangle}.$$

La segunda aseveración se deduce del desarrollo de $u_0/u_1$ en una fracción continuada simple finita, dada en la Sección 7.1, junto con la ecuación (7.4) y el Teorema 7.1.

**Problema**

1. Sean $a_0, a_1, \cdots, a_n$ y $b_0, b_1, \cdots, b_{n+1}$ enteros positivos ¿Cuáles son las condiciones para que

$$\langle a_0\ a_1, \cdots, a_n \rangle < \langle b_0, b_1, \cdots, b_{n+1} \rangle?$$

## 7.3 Fracciones continuadas infinitas

Sea $a_0, a_1, a_2, \cdots$ una sucesión infinita de enteros, todos positivos excepto tal vez $a_0$. Definimos inductivamente dos sucesiones de enteros $\{h_n\}$ y $\{k_n\}$ del modo siguiente:

$$
\begin{aligned}
(7.6) \qquad & h_{-2} = 0, \quad h_{-1} = 1, \quad h_i = a_i h_{i-1} + h_{i-2} \quad \text{para } i \geqq 0, \\
& k_{-2} = 1, \quad k_{-1} = 0, \quad k_i = a_i k_{i-1} + k_{i-2} \quad \text{para } i \geqq 0.
\end{aligned}
$$

Se observa que $k_0 = 1$, $k_1 = a_1 k_0 \geqq k_0$, $k_2 > k_1$, $k_3 > k_2$, etc., de modo que $1 = k_0 \leqq k_1 < k_2 < k_3 < \cdots < k_n < \cdots$.

**Teorema 7.3** *Para cualquier número real positivo x,*

$$\langle a_0, a_1, \cdots, a_{n-1}, x\rangle = \frac{xh_{n-1} + h_{n-2}}{xk_{n-1} + k_{n-2}}.$$

*Demostración.* Si $n = 0$, el resultado se interpreta como

$$x = \frac{xh_{-1} + h_{-2}}{xk_{-1} + k_{-2}},$$

lo cual es verdadero con base en las ecuaciones (7.6). Si $n = 1$, el resultado es

$$\langle a_0, x\rangle = \frac{xh_0 + h_{-1}}{xk_0 + k_{-1}},$$

lo cual puede verificarse a partir de (7.6) y el hecho de que $\langle a_0, x\rangle$ representa $a_0 + 1/x$. El teorema, en general, se establece por inducción. Suponiendo que el resultado se cumple para $\langle a_0, a_1, \cdots, a_{n-1}, x\rangle$, se ve que

$$
\begin{aligned}
\langle a_0, a_1, \cdots, a_n, x\rangle &= \left\langle a_0, a_1, \cdots, a_{n-1}, a_n + \frac{1}{x}\right\rangle \\
&= \frac{(a_n + 1/x)h_{n-1} + h_{n-2}}{(a_n + 1/x)k_{n-1} + k_{n-2}} \\
&= \frac{x(a_n h_{n-1} + h_{n-2}) + h_{n-1}}{x(a_n k_{n-1} + k_{n-2}) + k_{n-1}} = \frac{xh_n + h_{n-1}}{xk_n + k_{n-1}}.
\end{aligned}
$$

**Teorema 7.4** *Si se define* $r_{\text{n}} = \langle a_1, a_1, \cdots ; a_n\rangle$ *para todos los enteros* $n \geqq 0$, *entonces* $r_n = h_n/k_n$.

*Demostración.* Apliquemos el Teorema 7.3 con $x$ reemplazada por $a_n$ y a continuación usemos las ecuaciones (7.6), así que:

$$r_n = \langle a_0, a_1, \cdots, a_n\rangle = \frac{a_n h_{n-1} + h_{n-2}}{a_n k_{n-1} + k_{n-2}} = \frac{h_n}{k_n}.$$

**Teorema 7.5** *Las ecuaciones*

$$h_i k_{i-1} - h_{i-1} k_i = (-1)^{i-1} \text{ y } r_i - r_{i-1} = \frac{(-1)^{i-1}}{k_i k_{i-1}}$$

*se cumplen para* $i \geqq 1$. *Las identidades*

$$h_i k_{i-2} - h_{i-2} k_i = (-1)^i a_i \text{ y } r_i - r_{i-2} = \frac{(-1)^i a_i}{k_i k_{i-2}}$$

*se cumplen para* $i \geqq 2$. *La fracción* $h_i/k_i$ *es reducida, esto es* $(h_i, k_i) = 1$.

*Demostración.* Las ecuaciones (7.6) implican que $h_{-1}k_{-2} - h_{-2}k_{-1} = 1$. Continuando la demostración por inducción, se supone que $h_{i-1}k_{i-2} - h_{i-2}k_{i-1} = (-1)^{i-2}$. Una vez más se aplican las ecuaciones (7.6) para obtener $h_i k_{i-1} - h_{i-1}k_i = (a_i h_{i-1} + h_{i-2})k_{i-1} - h_{i-1}(a_i k_{i-1} + k_{i-2}) = -(h_{i-1}k_{i-2} - h_{i-2}k_{i-1}) = (-1)^{i-1}$. Esto prueba el primer resultado establecido en el teorema. Se divide por $k_{i-1}k_i$ para obtener el segundo resultado, la fórmula para $r_i - r_{i-1}$. Además, la fracción $h_i/k_i$ está en su más simple expresión dado que cualquier factor de $h_i$ y $k_i$ también es un factor de $(-1)^{i-1}$.

Las demás fórmulas pueden deducirse prácticamente en la misma forma a partir de (7.6), aunque en este caso no se requiere la inducción. Primero obsérvese que $h_0 k_{-2} - h_{-2}k_0 = a_0$ y que, en general, $h_i k_{i-2} - h_{i-2}k_i = (a_i h_{i-1} + h_{i-2})k_{i-2} - h_{i-2}(a_i k_{i-1} + k_{i-2}) = a_i(h_{i-1}k_{i-2} - h_{i-2}k_{i-1}) = (-1)^i a_i$. La identidad final puede obtenerse dividiendo por $k_{i-2}k_i$.

**Teorema 7.6** *Los valores* $r_n$ *definidos en el Teorema* 7.4 *satisfacen la cadena infinita de desigualdades* $r_0 < r_2 < r_4 < r_6 < \cdots < r_7 < r_5 < r_3 < r_1$. *Establecido en palabras, los* $r_n$ *con subíndices pares forman una sucesión creciente, aquellos con subíndices impares forman una sucesión decreciente y todo* $r_{2n}$ *es menor que todo* $r_{2j-1}$. *Además* $\lim_{n\to\infty} r_n$ *existe y para todo* $j \geqq 0$, $r_{2j} < \lim_{n\to\infty} r_n < r_{2j+1}$.

*Demostración.* Las identidades del Teorema 7.5 para $r_i - r_{i-1}$ y $r_i - r_{i-2}$ implican que $r_{2j} < r_{2j+2}$, $r_{2j-1} > r_{2j+1}$ y $r_{2j} < r_{2j-1}$ debido a que los $k_i$ son positivos para $i \geqq 0$ y los $a_i$ son positivos para $i \geqq 1$. Así se tiene $r_0 < r_2 < r_4 < \cdots$ y $r_1 > r_3 > r_5 > \cdots$. Para probar que $r_{2n} < r_{2j-1}$, se ponen los resultados anteriores juntos en la forma

$$r_{2n} < r_{2n+2j} < r_{2n+2j-1} \leqq r_{2j-1}.$$

La sucesión $r_0, r_2, r_4, \cdots$ es creciente monótona y acotada superiormente por $r_1$ y, por lo tanto, tiene un límite. Análogamente, la sucesión $r_1, r_3, r_5, \cdots$ es decreciente monótona y acotada inferiormente por $r_0$ y, por lo tanto, tiene un límite. Estos dos límites son iguales debido a que, por el Teorema 7.5, la diferencia $r_i - r_{i-1}$ tiende hacia cero conforme $i$ tiende al infinito, dado que los enteros $k_i$ son crecientes con $i$. Otra forma de mirar esto es observando que $(r_0, r_1)$, $(r_2, r_3)$, $(r_4, r_5)$, $\cdots$

es una cadena de intervalos anidados definiendo un número real, a saber $\lim_{n\to\infty} r_n$.

Estos teoremas sugieren la definición siguiente.

**Definición 7.1** *Una sucesión infinita $a_0, a_1, a_2, \cdots$ de enteros, todos positivos excepto tal vez $a_0$, determina una función continuada simple infinita $\langle a_0, a_1, a_2, \cdots\rangle$. El valor de $\langle a_0, a_1, a_2, \cdots\rangle$ está definido como* $\lim_{n\to\infty} \langle a_0, a_1, a_2, \cdots, a_n\rangle$.

Este límite, siendo el mismo que $\lim_{n\to\infty} r_n$ existe por el Teorema 7.6. Otra forma de escribir este límite es $\lim_{n\to\infty} h_n/k_n$. El número racional $\langle a_0, a_1, \cdots, a_n\rangle = h_n/k_n = r_n$ se llama el $n$-ésimo convergente a la fracción continuada infinita. Se dice que la fracción continuada infinita converge al valor $\lim_{n\to\infty} r_n$. En el caso de una fracción continuada simple finita $\langle a_0, a_1, \cdots, a_n\rangle$, al número $\langle a_0, a_1, \cdots, a_m\rangle$. se le da el nombre de $m$-ésimo convergente a $\langle a_0, a_1, \cdots, a_n\rangle$.

**Teorema 7.7** *El valor de cualquier fracción continuada simple infinita $\langle a_0, a_1, a_2, \cdots\rangle$ es irracional.*

*Demostración.* Escribiendo $\theta$ por $\langle a_0, a_1, a_2, \cdots\rangle$ se observa, por el Teorema 7.6, que $\theta$ se encuentra entre $r_n$ y $r_{n+1}$, de manera que $0 < |\theta - r_n| < |r_{n+1} - r_n|$. Multiplicando por $k_n$ y haciendo uso del resultado del Teorema 7.5 de que $|r_{n+1} - r_n| = (k_n k_{n+1})^{-1}$, se tiene

$$0 < |k_n\theta - h_n| < \frac{1}{k_{n+1}}.$$

Ahora supóngase que $\theta$ fuera racional, digamos $\theta = a/b$ con los enteros $a$ y $b$, $b > 0$. Entonces la desigualdad anterior se transformaría, después de multiplicarla por $b$, en

$$0 < |k_n a - h_n b| < \frac{b}{k_{n+1}}.$$

Los enteros $k_n$ crecen con $n$, de manera que se escogería $n$ lo suficientemente grande de manera que $b < k_{n+1}$. Entonces el entero $|k_n a - h_n b|$ estaría entre 0 y 1, lo cual es imposible.

Supóngase que se tienen dos fracciones continuadas simples infinitas diferentes, $\langle a_0, a_1, a_2, \cdots\rangle$ y $\langle b_0, b_1, b_2, \cdots\rangle$. ¿Pueden converger éstas al mismo valor? La respuesta es no y esto se establece en los dos resultados siguientes

**Lema 7.8** *Sea $\theta = \langle a_1, a_1, a_2 \cdots\rangle$. Entonces $a_0 = [\theta]$. Además si $\theta_1$ denota a $\langle a_1, a_2, a_3, \cdots\rangle$ entonces $\theta = a_0 + 1/\theta_1$.*

*Demostración.* Por el Teorema 7.6 se ve que $r_0 < \theta < r_1$, esto es $a_0 < \theta < a_0 + 1/a_1$. Ahora bien $a_1 \geqq 1$, de manera que se tiene $a_0 < \theta < a_0 + 1$ y de aquí que $a_0 = [\theta]$. También

$$\theta = \lim_{n\to\infty} \langle a_0, a_1, \cdots, a_n\rangle = \lim_{n\to\infty}\left(a_0 + \frac{1}{\langle a_1, \cdots, a_n\rangle}\right)$$

$$= a_0 + \frac{1}{\lim_{n\to\infty}\langle a_1, \cdots, a_n\rangle} = a_0 + \frac{1}{\theta_1}.$$

**Teorema 7.9** *Dos fracciones continuadas simples infinitas distintas convergen a valores diferentes.*

*Demostración.* Supongamos que $\langle a_0, a_1, a_2, \cdots\rangle = \langle b_0, b_1, b_2, \cdots\rangle = \theta$. Entonces, por el Lema 7.8, $[\theta] = a_0 = b_0$ y

$$\theta = a_0 + \frac{1}{\langle a_1, a_2, \cdots\rangle} = b_0 + \frac{1}{\langle b_1, b_2, \cdots\rangle}.$$

De aquí que $\langle a_1, a_2, \cdots\rangle = \langle b_1, b_2, \cdots\rangle$. La repetición del argumento da $a_1 = b_1$ y así por inducción matemática, $a_n = b_n$ para todo $n$.

**Problemas**

1. Evaluar la fracción continuada infinita $\langle 1, 1, 1, 1, \cdots\rangle$. *Sugerencia*: mediante el Lema 7.8, se ve que, en este caso, $\theta = 1 + 1/\theta$. Esto proporciona una ecuación cuadrática, de cuyas raíces sólo una es positiva.
2. Evaluar las fracciones continuadas infinitas $\langle 2, 1, 1, 1, 1, \cdots\rangle$ y $\langle 2, 3, 1, 1, 1, 1, \cdots\rangle$. *Sugerencia*: aplicar el resultado del problema anterior en conjunción con el Lema 7.8
3. Evaluar las fracciones continuadas infinitas:
   *a*) $\langle 2, 2, 2, 2, \cdots\rangle$;
   *b*) $\langle 1, 2, 1, 2, 1, 2, \cdots\rangle$;
   *c*) $\langle 2, 1, 2, 1, 2, 1, \cdots\rangle$;
   *d*) $\langle 1, 3, 1, 2, 1, 2, 1, 2, \cdots\rangle$.
4. Para $n \geqq 1$, probar que $k_n/k_{n-1} = \langle a_n, a_{n-1} \cdots, a_2, a_1\rangle$. Encontrar y probar un desarrollo fraccionario continuado semejante para $h_n/h_{n-1}$.

## 7.4 Números irracionales

Se ha demotrado que toda fracción continuada simple infinita representa un número irracional. Inversamente, si se empieza con un número irracional $\xi$, o bien $\xi_0$, puede desarrollarse en una fracción continuada simple infinita. Para hacerlo se define $a_0 = [\xi_0]$, $\xi_1 = 1/(\xi_0 - a_0)$ y en seguida $a_1 = [\xi_1]$, $\xi_2 = 1/(\xi_1 - a_1)$ y así, mediante una definición inductiva

$$(7.7) \qquad a_i = [\xi_i], \qquad \xi_{i+1} = \frac{1}{\xi_i - a_i}.$$

Por definición, los $a_i$ son enteros y los $\xi_i$ son todos irracionales puesto que la irracionalidad de $\xi_1$ es consecuencia de la de $\xi_0$, la de $\xi_2$ por la de $\xi_1$, y así sucesivamente. Además, $a_i \geqq 1$ para $i \geqq 1$ debido a que $a_{i-1} = [\xi_{i-1}]$ y el hecho de que $\xi_{i-1}$ es irracional implica que

$$a_{i-1} < \xi_{i-1} < 1 + a_{i-1}, \quad 0 < \xi_{i-1} - a_{i-1} < 1,$$

$$\xi_i = \frac{1}{\xi_{i-1} - a_{i-1}} > 1, \quad a_i = [\xi_i] \geqq 1.$$

A continuación se hace la aplicación repetida de (7.7) en la forma $\xi_i = a_i + 1/\xi_{i+1}$ para obtener la cadena

$$\xi = \xi_0 = a_0 + \frac{1}{\xi_1} = \langle a_0, \xi_1 \rangle$$

$$= \left\langle a_0, a_1 + \frac{1}{\xi_2} \right\rangle = \langle a_0, a_1, \xi_2 \rangle$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$= \left\langle a_0, a_1, \cdots, a_{m-2}, a_{m-1} + \frac{1}{\xi_m} \right\rangle = \langle a_0, a_1, \cdots, a_{m-1}, \xi_m \rangle.$$

Esto sugiere, pero no establece, que $\xi$ es el valor de la fracción continuada infinita $\langle a_0, a_1, a_2, \cdots \rangle$ determinada por los enteros $a_i$.

Para probar esto se aplica el Teorema 7.3 para escribir

$$(7.8) \qquad \xi = \langle a_0, a_1, \cdots, a_{n-1}, \xi_n \rangle = \frac{\xi_n h_{n-1} + h_{n-2}}{\xi_n k_{n-1} + k_{n-2}}$$

con los $h_i$ y $k_i$ definidos como en (7.6). Por el Teorema 7.5 se obtiene

$$(7.9) \quad \xi - r_{n-1} = \xi - \frac{h_{n-1}}{k_{n-1}} = \frac{\xi_n h_{n-1} + h_{n-2}}{\xi_n k_{n-1} + k_{n-2}} - \frac{h_{n-1}}{k_{n-1}}$$

$$= \frac{-(h_{n-1}k_{n-2} - h_{n-2}k_{n-1})}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})} = \frac{(-1)^{n-1}}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})}.$$

Esta fracción tiende hacia cero conforme $n$ tiende al infinito debido a que los enteros $k_n$ son crecientes con $n$ y $\xi_n$ es positivo. De aquí que $\xi - r_{n-1}$ tiende hacia cero conforme $n$ tiende al infinito y entonces, por lo Definición 7.1,

$$\xi = \lim_{n\to\infty} r_n = \lim_{n\to\infty} \langle a_0, a_1, \cdots, a_n \rangle = \langle a_0, a_1, a_2, \cdots \rangle.$$

Resumiremos los resultados de las dos últimas secciones en el siguiente teorema.

**Teorema 7.10** *Cualquier número irracional $\xi$ es expresable unívocamente, mediante el procedimiento que dieron las ecuaciones* (7.7), *como una fracción continuada simple infinita $\langle a_0, a_1, a_2, \cdots \rangle$. Inversamente, cualquier fracción continuada determinada por los enteros $a_i$ los cuales son positivos para todo $i > 0$ representa un número irracional, $\xi$. La fracción continuada simple finita $\langle a_0, a_1, \cdots, a_n \rangle$ tiene el valor racional $h_n/k_n = r_n$ y recibe el nombre de $n$-ésimo convergente a $\xi$. Las ecuaciones* (7.6) *relacionan los $h_i$ y los $k_i$ a los $a_i$. Para $n = 0$, 2, 4, $\cdots$ estos convergentes forman una sucesión creciente monótona con $\xi$ como límite. De modo semejante, para $n = 1$, 3, 5, $\cdots$ los convergentes forman una sucesión decreciente monótona que tiende hacia $\xi$. Los denominadores $k_n$ de los convergentes son una sucesión creciente de enteros positivos para $n > 0$. Finalmente, con $\xi_i$ definido por* (7.7), *se tiene $\langle a_0, a_1, \cdots \rangle = \langle a_0, a_1, \cdots a_{n-1}, \xi_n \rangle$ y $\xi_n = \langle a_n, a_{n+1}, a_{n+2}, \cdots \rangle$.*

*Demostración.* Sólo la última ecuación es nueva y se vuelve obvia si se aplica a $\xi_n$ *el* proceso descrito al principio de esta sección.

**Problemas**

1. Desarrolle cada una de los siguientes como fracciones continuadas simples infinitas $\sqrt{2}$, $\sqrt{2} - 1$, $\sqrt{2}/2$, $\sqrt{3}$, $1/\sqrt{3}$.
2. Dado que dos números irracionales tienen convergentes idénticos $h_0/k_0$, $h_1/k_1, \cdots$ hasta $h_n/k_n$, probar que sus desarrollos fraccionarios continuados son idénticos hasta $a_n$.
3. Sean $\alpha$, $\beta$, $\gamma$ números irracionales que satisfacen $\alpha < \beta < \gamma$. Si $\alpha$ y $\gamma$ tienen convergentes idénticos $h_0/k_0$, $h_1/k_1, \cdots$ hasta $h_n/k_n$ probar que $\beta$ también tiene estos mismos convergentes hasta $h_n/k_n$.
4. Sea $\xi$ un número irracional con desarrollo fraccionario continuado $\langle a_0, a_1, a_2, a_3, \ldots \rangle$. Sea $b_1, b_2, b_3, \ldots$ cualquier sucesión finita o bien infinita de enteros positivos. Probar que
$$\lim_{n\to\infty} \langle a_0, a_1, a_2, \cdots, a_n, b_1, b_2, b_3, \cdots \rangle = \xi.$$
5. Con la notación usada en el texto, probar que
$$\xi_n = \langle a_n, a_{n+1}, a_{n+2}, \cdots \rangle.$$
6. Probar que para $n \geqq 1$,
$$\xi - \frac{h_n}{k_n} = (-1)^n k_n^{-2} \{\xi_{n+1} + \langle 0, a_n, a_{n-1}, \cdots a_2, a_1 \rangle\}^{-1}.$$
7. Probar que
$$k_n |k_{n-1}\xi - h_{n-1}| + k_{n-1} |k_n \xi - h_n| = 1.$$

## 7.5 Aproximaciones para números irracionales

Continuando con la misma notación de las secciones anteriores, ahora se demostrará que los convergentes $k_n/k_n$ forman una sucesión de las "mejores" aproximaciones racionales para el número irracional $\xi$.

**Teorema 7.11** *Para cualquier* $n \geqq 0$, *se tiene*

$$\left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{k_n k_{n+1}} \quad y \quad |\xi k_n - h_n| < \frac{1}{k_{n+1}}.$$

*Demostración.* La segunda desigualdad se deduce de la primera multiplicando por $k_n$. Por (7.9) y (7.7) se ve que

$$\left|\xi - \frac{h_n}{k_n}\right| = \frac{1}{k_n(\xi_{n+1}k_n + k_{n-1})} < \frac{1}{k_n(a_{n+1}k_n + k_{n-1})}.$$

Aplicando (7.6); se reemplaza $a_{n+1}k_n + k_{n-1}$ por $k_{n+1}$ para obtener la primera desigualdad.

**Teorema 7.12** *Los convergentes* $h_n/k_n$ *son sucesivamente más próximos a* $\xi$, *esto es*

$$\left|\xi - \frac{h_n}{k_n}\right| < \left|\xi - \frac{h_{n-1}}{k_{n-1}}\right|.$$

*De hecho, se cumple la desigualdad más fuerte* $|\xi k_n - h_n| < |\xi k_{n-1} - h_{n-1}|$.

*Demostración.* Para ver que la segunda desigualdad es más fuerte en el sentido de que implica la primera, apliquemos $k_{n-1} \leqq k_n$ para escribir

$$\left|\xi - \frac{h_n}{k_n}\right| = \frac{1}{k_n}|\xi k_n - h_n| < \frac{1}{k_n}|\xi k_{n-1} - h_{n-1}|$$
$$\leqq \frac{1}{k_{n-1}}|\xi k_{n-1} - h_{n-1}| = \left|\xi - \frac{h_{n-1}}{k_{n-1}}\right|.$$

Ahora, para probar la desigualdad más fuerte, se observa que $a_n + 1 > \xi_n$, por (7.7), y así por (7.6),

$$\xi_n k_{n-1} + k_{n-2} < (a_n + 1)k_{n-1} + k_{n-2}$$
$$= k_n + k_{n-1} \leqq a_{n+1}k_n + k_{n-1} = k_{n+1}.$$

Esta desigualdad y (7.9) implican que

$$\left|\xi - \frac{h_{n-1}}{k_{n-1}}\right| = \frac{1}{k_{n-1}(\xi_n k_{n-1} + k_{n-2})} > \frac{1}{k_{n-1}k_{n+1}}.$$

Multipliquemos por $k_{n-1}$ y apliquemos el Teorema 7.11 para obtener

$$|\xi k_{n-1} - h_{n-1}| > \frac{1}{k_{n+1}} > |\xi k_n - h_n|.$$

El convergente $h_n/k_n$ es la mejor aproximación para $\xi$ de todas las fracciones racionales con denominador $k_n$ o menor. El teorema siguiente establece esto de manera diferente.

**Teorema 7.13** *Si $a/b$ es un número racional con denominador positivo tal que $|\xi - a/b| < |\xi - h_n/k_n|$ para algún $n \geqq 1$, entonces $b > k_n$. De hecho, si $|\xi b - a| < |\xi k_n - h_n|$ para algún $n \geqq 0$, entonces $b \geqq k_{n+1}$.*

*Demostración.* Primero se demostrará que la segunda parte del teorema implica la primera. Supóngase que la primera parte es falsa de modo que hay un $a/b$ con

$$\left|\xi - \frac{a}{b}\right| < \left|\xi - \frac{h_n}{k_n}\right| \text{ y } b \leqq k_n.$$

El producto de estas desigualdades da $|\xi b - a| < |\xi k_n - h_n|$. Pero la segunda parte del teorema dice que esto implica $b \geqq k_{n+1}$, de modo que se tiene una contradicción, dado que $k_n < k_{n+1}$ para $n \geqq 1$.

Para probar la segunda parte del teorema se procede nuevamente mediante un argumento indirecto, suponiendo que $|\xi b - a| < |\xi k_n - h_n|$ y $b < k_{n+1}$. Considérense las ecuaciones lineales en $x$ y $y$,

$$xk_n + yk_{n+1} = b, \qquad xh_n + yh_{n+1} = a.$$

Por el Teorema 7.5, el determinante de los coeficientes es $y$, en consecuencia, estas ecuaciones tienen una solución entera $x$, $y$. Es más, ni $x$ ni $y$ son cero. Porque si $x = 0$ entonces $b = yk_{n+1}$, lo cual implica que $y \neq 0$, de hecho que $y > 0$ y $b \geqq k_{n+1}$, en contradicción a $b < k_{n-1}$. Si $y = 0$ entonces $a = xh_n$, $b = xk_n$ y

$$|\xi b - a| = |\xi xk_n - xh_n| = |x|\,|\xi k_n - h_n| \geqq |k_n\xi - h_n|$$

dado que $|x| \geqq 1$, y una vez más se tiene una contradicción.

A continuación se probará que $x$ y $y$ tienen signos opuestos. Primero, si $y < 0$, entonces $xk_n = b - yk_{n+1}$ muestra que $x > 0$. Segundo, si $y > 0$, entonces $b < k_{n+1}$ implica que $b < yk_{n+1}$ y, por tanto $xk_n$ es negativo, de donde $x < 0$. Ahora, del Teorema 7.10, se deduce que $\xi k_n - h_n$ y $\xi k_{n+1} - h_{n+1}$ tienen signos opuestos y de aquí que $x(\xi k_n - h_n)$ y $y(\xi k_{n+1} - h_{n+1})$ tienen el mismo signo. A partir de las ecuaciones que definen a $x$ y $y$ se obtiene $\xi b - a = x(\xi k_n - h_n) + y(\xi k_{n+1} - h_{n+1})$. Dado que los dos términos de la derecha tienen el mismo signo, el valor absoluto de todo es igual a la suma de los valores absolutos separados. Así que

$$\begin{aligned} |\xi b - a| &= |x(\xi k_n - h_n) + y(\xi k_{n+1} - h_{n+1})| \\ &= |x(\xi k_n - h_n)| + |y(\xi k_{n+1} - h_{n+1})| \\ &> |x(\xi k_n - h_n)| = |x|\,|\xi k_n - h_n| \geq |\xi k_n - h_n|. \end{aligned}$$

Esto es una contradicción y así, queda establecido el teorema.

**Teorema 7.14** *Denotemos por $\xi$ cualquier número irracional. Si existe un número racional $a/b$ con $b \geqq 1$ tal que*

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

*entonces $a/b$ es igual a uno de los convergentes del desarrollo fraccionario continuado simple de $\xi$.*

*Demostración.* Es suficiente con demostrar el resultado en el caso $(a, b) = 1$. Sean $h_j/k_j$ los convergentes del desarrollo fraccionario continuado simple de $\xi$ y supóngase que $a/b$ no es un convergente. Las desigualdades $k_n \leqq b < k_{n+1}$ determinan un entero $n$. Debido al Teorema 7.13, la desigualdad $|\xi b - a| < |\xi k_n - b_n|$ es imposible para este $n$. Por lo tanto, se tiene

$$|\xi k_n - h_n| \leqq |\xi b - a| < \frac{1}{2b},$$

$$\left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{2bk_n}.$$

Aplicando los hechos de que $a/b \neq h_n/k_n$ y de que $bh_n - ak_n$ es un entero, se encuentra que

$$\frac{1}{bk_n} \leqq \frac{|bh_n - ak_n|}{bk_n} = \left|\frac{h_n}{k_n} - \frac{a}{b}\right| \leqq \left|\xi - \frac{h_n}{k_n}\right| + \left|\xi - \frac{a}{b}\right| < \frac{1}{2bk_n} + \frac{1}{2b^2}.$$

Esto implica $b < k_n$ lo cual es una contradicción.

**Teorema 7.15** *El $n$-*ésimo *convergente de $1/x$ es el recíproco del $(n - 1)$*-ésimo *convergente de $x$ si $x$ es cualquier número real $> 1$.*

*Demostración.* Se tiene $x = \langle a_0, a_1, \cdots\rangle$ y $1/x = \langle 0, a_0, a_1, \cdots\rangle$. Si $h_n/k_n$ y $h'_n/k'_n$ son los convergentes para $x$ y $1/x$, respectivamente, entonces

$$\begin{aligned}
&h'_0 = 0, \quad h'_1 = 1, \quad h'_2 = a_1, \qquad && h'_n = a_{n-1}h'_{n-1} + h'_{n-2}\\
&\phantom{h'_0 = 0, \quad} k_0 = 1, \quad k_1 = a_1, && k_{n-1} = a_{n-1}k_{n-2} + k_{n-3}\\
&k'_0 = 1, \quad k'_1 = a_0, \quad k'_2 = a_0a_1 + 1, && k'_n = a_{n-1}k'_{n-1} + k'_{n-2}\\
&\phantom{k'_0 = 1, \quad} h_0 = a_0, \quad h_1 = a_0a_1 + 1, && h_{n-1} = a_{n-1}h_{n-2} + h_{n-3}.
\end{aligned}$$

Ahora, el teorema se concluye por inducción matemática.

**Problemas**

1. Probar que la primera aseveración del Teorema 7.13 se cumple en el caso de que $n = 0$ si $k_1 > 1$.

2. Probar que la primera aseveración del Teorema 7.13 se vuelve falsa si "$b > k_n$" se reemplaza por "$b \geqq k_{n+1}$". *Sugerencia:* usar $\xi = \pi^{-1}$ y $n = 1$.
3. Decimos que un número racional $a/b$ con $b > 0$ es una "buena aproximación" para el número irracional $\xi$ si

$$|\xi b - a| = \min_{\substack{\text{todo } x \\ 0<y\leqq b}} |\xi y - x|,$$

donde, como se indica, el mínimo del segundo miembro se toma sobre todos los enteros $x$ y todos los $y$ que satisfacen $0 < y \leqq b$. Probar que todo convergente a $\xi$ es una "buena aproximación".
4. Probar que toda "buena aproximación" para $\xi$ es un convergente.
5. *a*) Probar que si $r/s$ se encuentra entre $a/b$ y $c/d$, donde los denominadores de estas fracciones racionales son positivos, y si $ad - bc = \pm 1$, entonces $s > b$ y $s > d$.

   *b*) Sea $\xi$ un irracional con convergentes $\{h_n/k_n\}$. Probar que la sucesión

$$\frac{h_{n-1}}{k_{n-1}}, \frac{h_{n-1}+h_n}{k_{n-1}+k_n}, \frac{h_{n-1}+2h_n}{k_{n-1}+2k_n}, \cdots, \frac{h_{n-1}+a_{n+1}h_n}{k_{n-1}+a_{n+1}k_n} = \frac{h_{n+1}}{k_{n+1}}$$

   es creciente si $n$ es impar, decreciente si $n$ es par. Si $a/b$ y $c/d$ denotan cualquier par consecutivo de esta sucesión, probar que $ad - bc = \pm 1$. Los términos de esta sucesión, excepto el primero y el último, se llaman los convergentes secundarios; aquí $n$ recorre todos los valores $0, 1, 2, \cdots$.

   *c*) Decimos que un número racional $a/b$ es una "aproximación regular" para $\xi$ si $|\xi - a/b| = \min |\xi - x/y|$, tomando el mínimo sobre todos los enteros $x$ y $y$ con $0 > y \leqq b$. Probar que toda buena aproximación es una aproximación regular. Probar que toda aproximación regular es un convergente o bien un convergente secundario para $\xi$.

   *d*) Probar que no todo convergente secundario es una "aproximación regular". *Sugerencia*: considerar $\xi = \sqrt{2}$.

   *e*) Decimos que una sucesión infinita de números racionales, $r_1, r_2, r_3, \cdots$ con límite $\xi$ es una "sucesión de apoximación" para un número irracional $\xi$ si $|\xi - r_{j+1}| < |\xi - r_j|, j = 1, 2, 3, \cdots$ y si los denominadores positivos de los $r_j$ son crecientes con $j$. Probar que las "aproximaciones regulares" para $\xi$ forman una "sucesión de aproximación".

   *f*) Denotemos por $S_{n-1}$ la sucesión finita de (*b*) con el primer término eliminado, de modo que $S_{n-1}$ tiene $a_{n+1}$ términos, siendo el último término $h_{n+1}/k_{n+1}$. Probar que la sucesión infinita de números racionales obtenida tomando primero los términos de $S_0$ en orden, después los términos de $S_2$, después los de $S_4$, después los de $S_6$, $\cdots$, también es "una sucesión de aproximación" para $\xi$. Probar también que esta sucesión es máxima en el sentido de que si se introduce cualquier otro número racional $< \xi$ en la sucesión como un nuevo miembro, no se tendrá una sucesión de aproximación.

   *g*) Establecer propiedades análogas para la sucesión obtenida tomando los términos de $S_{-1}, S_1, S_3, S_5, \cdots$.
6. Sea $\xi$ irracional, $\xi = \langle a_0, a_1, a_2, \cdots \rangle$. Verificar que

$$-\xi = \langle -a_0 - 1, 1, a_1 - 1, a_2, a_3, \cdots \rangle \text{ si } a_1 > 1$$

y $-\xi = \langle -a_0 - 1, a_2 + 1, a_3, a_4, \cdots \rangle$ si $a_1 = 1$.

## 7.6 Las mejores aproximaciones posibles

El Teorema 7.11 proporciona otro método de probar el Teorema 6.9. Porque en la proposición del Teorema 7.11 puede reemplazarse $k_{n+1}$ por el entero menor $k_n$ para obtener la desigualdad más débil, pero todavía correcta

$$\left|\xi - \frac{h_n}{k_n}\right| < \frac{1}{k_n^2}$$

Es más, el proceso descrito en la Sección 7.4 nos capacita para determinar, para cualquier irracional dado $\xi$, tantos convergentes $h_n/k_n$ como se deseen. También pueden aplicarse las fracciones continuadas en otras demostraciones de los Teoremas 6.11 y 6.12. Primero se dará un lema sencillo.

**Lema 7.16** *Si $x$ es real, $x > 1$, y $x + x^{-1} < \sqrt{5}$, entonces $x < \frac{1}{2}(\sqrt{5} + 1)$ y $x^{-1} > \frac{1}{2}(\sqrt{5} - 1)$.*

*Demostración.* Para el real $x \geqq 1$ se observa que $x + x^{-1}$ crece con $x$ y $x + x^{-1} = \sqrt{5}$ si $x = \frac{1}{2}(\sqrt{5} + 1)$.

**Teorema 7.17** (*Hurwitz*) *Dado cualquier número irracional $\xi$, existe un número infinito de números racionales $h/k$ tales que*

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{\sqrt{5}\,k^2}. \tag{7.13}$$

*Demostración.* Se establecerá que, de cada tres convergentes consecutivos del desarrollo fraccionario continuado simple de $\xi$, por lo menos uno satisface la desigualdad.

Denotemos $k_n/k_{n-1}$ por $q_n$. Primero se probará que

$$q_j + q_j^{-1} < \sqrt{5} \tag{7.14}$$

si (7.13) es falsa tanto para $h/k = h_{j-1}/k_{j-1}$ como para $h/k = h_j/k_j$. Supóngase que (7.13) es falsa para estos dos valores de $h/k$. Se tiene

$$\left|\xi - \frac{h_{j-1}}{k_{j-1}}\right| + \left|\xi - \frac{h_j}{k_j}\right| \geqq \frac{1}{\sqrt{5}\,k_{j-1}^2} + \frac{1}{\sqrt{5}\,k_j^2}.$$

Pero $\xi$ se encuentra entre $h_{j-1}/k_{j-1}$ y $h_j/k_j$ y de aquí que, aplicando el Teorema 7.5, se encuentra que

$$\left|\xi - \frac{h_{j-1}}{k_{j-1}}\right| + \left|\xi - \frac{h_j}{k_j}\right| = \left|\frac{h_{j-1}}{k_{j-1}} - \frac{h_j}{k_j}\right| = \frac{1}{k_{j-1}k_j}.$$

Combinando estos resultados se obtiene

$$\frac{k_j}{k_{j-1}} + \frac{k_{j-1}}{k_j} \leqq \sqrt{5}.$$

Dado que el primer miembro es racional, realmente se tiene una desigualdad estricta, y se concluye (7.14).

Ahora supóngase que (7.13) es falsa para $h/k = h_i/k_i$, $i = n - 1, n, n + 1$. Entonces se tiene (7.14) tanto para $j = n$ como para $j = n + 1$. Por el Lema 7.16 se ve que $q_n^{-1} > \frac{1}{2}(\sqrt{5} - 1)$ y $q_{n+1} < \frac{1}{2}(\sqrt{5} + 1)$, y, por (7.6), se encuentra que $q_{n+1} = a_{n+1} + q_n^{-1}$. Esto nos proporciona

$$\tfrac{1}{2}(\sqrt{5} + 1) > q_{n+1} = a_{n+1} + q_n^{-1} > a_{n+1} + \tfrac{1}{2}(\sqrt{5} - 1)$$
$$\geqq 1 + \tfrac{1}{2}(\sqrt{5} - 1) = \tfrac{1}{2}(\sqrt{5} + 1)$$

y esto es una contradicción.

**Teorema 7.18** *La constante* $\sqrt{5}$ *del teorema anterior es la mejor posible. En otras palabras, el Teorema 7.17 no se cumple si* $\sqrt{5}$ *se reemplaza por un valor mayor.*

*Demostración.* Basta presentar un número irracional $\xi$ para el cual $\sqrt{5}$ sea la constante mayor posible. Considérese el irracional $\xi$ cuyo desarrollo fraccionario continuado sea $\langle 1, 1, 1, \cdots \rangle$. Se ve que

$$\xi = 1 + \frac{1}{\langle 1, 1, \cdots \rangle} = 1 + \frac{1}{\xi}, \quad \xi^2 = \xi + 1, \quad \xi = \frac{1}{2}(\sqrt{5} + 1).$$

Aplicando (7.7) puede probarse por inducción que $\xi_i = (\sqrt{5} + 1)/2$ para todo $i \geqq 0$, porque si $\xi_i = (\sqrt{5} + 1)/2$ entonces

$$\xi_{i+1} = (\xi_i - a_i)^{-1} = (\tfrac{1}{2}(\sqrt{5} + 1) - 1)^{-1} = \tfrac{1}{2}(\sqrt{5} + 1).$$

Un cálculo sencillo proporciona $h_0 = k_0 = k_1 = 1$, $h_1 = k_2 = 2$. Las ecuaciones (7.6) se transforman en $h_i = h_{i-1} + h_{i-2}$, $k_i = k_{i-1} + k_{i-2}$, y por tanto, por inducción matemática, $k_n = h_{n-1}$ para $n \geqq 1$. De aquí que se tiene

$$\lim_{n\to\infty} \frac{k_{n-1}}{k_n} = \lim_{n\to\infty} \frac{k_{n-1}}{h_{n-1}} = \frac{1}{\xi} = \frac{\sqrt{5} - 1}{2},$$

$$\lim_{n\to\infty} \left(\xi_{n+1} + \frac{k_{n-1}}{k_n}\right) = \frac{\sqrt{5} + 1}{2} + \frac{\sqrt{5} - 1}{2} = \sqrt{5}.$$

Si $c$ es cualquier constante que excede a $\sqrt{5}$, entonces

$$\xi_{n+1} + \frac{k_{n-1}}{k_n} > c$$

se cumple sólo para un número finito de valores de $n$. Así que, por (7.9),

$$\left|\xi - \frac{h_n}{k_n}\right| = \frac{1}{k_n^2(\xi_{n+1} + k_{n-1}/k_n)} < \frac{1}{ck_n^2}$$

se cumple sólo para un número finito de valores de $n$. De donde sólo hay un número finito de números racionales $h/k$ que satisfacen $|\xi - h/k| < 1/(ck^2)$, debido a que, por el Teorema 7.14, cualquiera de esas $h/k$ es uno de los convergentes para $\xi$.

**Problemas**

1. Encontrar dos números racionales $a/b$ que satisfagan

$$\left|\sqrt{2} - \frac{a}{b}\right| < \frac{1}{\sqrt{5}\,b^2}$$

2. Encontrar dos números racionales $a/b$ que satisfagan

$$\left|\pi - \frac{a}{b}\right| < \frac{1}{\sqrt{5}\,b^2}.$$

3. Probar que lo siguiente es falso para cualquier constante $c > 2$: Dado cualquier número irracional $\xi$, existe un número infinito de números racionales $h/k$ tales que

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{k^c}.$$

4. Dada cualquier constante $c$, probar que existe un número irracional $\xi$ y un número infinito de números racionales $h/k$ tales que

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{k^c}.$$

5. Probar que cada dos convergentes consecutivos $h_n/k_n$ para $\xi$ con $n \geqq 0$, por lo menos uno satisface

$$\left|\xi - \frac{h}{k}\right| < \frac{1}{2k^2}.$$

*Sugerencia*: aplicar el Lema 7.16.

## 7.7 Fracciones continuadas periódicas

Se dice que una fracción continuada simple infinita $\langle a_0, a_1, a_2, \cdots\rangle$ es periódica si existe un entero $n$ tal que $a_r = a_{n+r}$ para todos los enteros $r$ suficientemente grandes. Por lo tanto, una fracción continuada periódica puede escribirse en la forma

$$(7.15)\quad \langle b_0, b_1, b_2, \cdots, b_j, a_0, a_1, \cdots, a_{n-1}, a_0, a_1, \cdots, a_{n-1}, \cdots\rangle$$
$$= \langle b_0, b_1, b_2, \cdots, b_j, \overline{a_0, a_1, \cdots, a_{n-1}}\rangle,$$

donde la raya sobre los $a_0, a_1, \cdots, a_{n-1}$ indica que este bloque de enteros se repite indefinidamente. Por ejemplo, $\langle\overline{2, 3}\rangle$ denota $\langle 2, 3, 2, 3, 2, 3, \cdots\rangle$ y su valor se calcula fácilmente. Escribiendo $\theta$ por $\langle\overline{2, 3}\rangle$ se tiene

$$\theta = 2 + \cfrac{1}{3 + \cfrac{1}{\theta}}.$$

Esta es una ecuación cuadrática en $\theta$ y se descarta la raíz negativa para obtener el valor $\theta = (3 + \sqrt{15})/3$. Como segundo ejemplo considérese $\langle 4, 1, \overline{2, 3},\rangle$. Llamándolo $\xi$ se tiene $\xi = \langle 4, 1, \theta\rangle$, con $\theta$ como en el anterior, y así

$$\xi = 4 + (1 + \theta^{-1})^{-1} = 4 + \frac{\theta}{\theta + 1} = \frac{29 + \sqrt{15}}{7}.$$

Estos dos ejemplos ilustran el siguiente resultado.

**Teorema 7.19** *Toda fracción continuada simple periódica es un número irracional cuadrático, e inversamente.*

*Demostración.* Escribamos $\xi$ por la fracción continuada periódica de (7.15) y $\theta$ por su parte puramente periódica, $\theta = \langle\overline{a_0, a_1, \cdots, a_{n-1}}\rangle = \langle a_0, a_1, \cdots, a_{n-1}, \theta\rangle$. Entonces la ecuación (7.8) nos da

$$\theta = \frac{\theta h_{n-1} + h_{n-2}}{\theta k_{n-1} + k_{n-2}},$$

y esta es una ecuación cuadrática en $\theta$. De aquí que $\theta$ es un número irracional cuadrático o bien un número racional pero, por el Teorema 7.7, lo último queda excluido. Ahora $\xi$ puede escribirse en términos de $\theta$,

$$\xi = \langle b_0, b_1, \cdots, b_j, \theta\rangle = \frac{\theta m + m'}{\theta q + q'}$$

donde $m'/q'$ y $m/q$ son los dos últimos convergentes para $\langle b_0, b_1, \cdots b_j\rangle$. Pero $\theta$ es de la forma $(a + \sqrt{b})/c$ y de aquí que $\xi$ es de forma semejante debido a que, como con $\theta$, puede excluirse la posibilidad de que $\xi$ sea racional.

Para probar lo inverso, empecemos con cualquier irracional cuadrático $\xi$, o bien $\xi_0$, de la forma $\xi = \xi_0 = (a + \sqrt{b})/c$, con los enteros $a, b, c, d > 0$, $c \neq 0$. El entero $b$ no es un cuadrado perfecto puesto que $\xi$ es irracional. Multipliquemos el numerador y el denominador por $|c|$ para obtener

$$\xi_0 = \frac{ac + \sqrt{bc^2}}{c^2} \text{ o bien } \xi_0 = \frac{-ac + \sqrt{bc^2}}{-c^2}$$

de acuerdo conque $c$ sea positiva o bien negativa. Así puede escribirse $\xi$ en la forma

$$\xi_0 = \frac{m_0 + \sqrt{d}}{q_0}$$

donde $q_0 | (d - m_0^2)$, $d$, $m_0$ y $q_0$ son enteros, $q_0 \neq 0$, $d$ no es un entero cuadrado perfecto. Escribiendo $\xi_0$ en esta forma puede obtenerse una formulación sencilla de su desarrollo fraccionario continuado $\langle a_0, a_1, a_2, \cdots \rangle$. Se probará que las ecuaciones

$$(7.16) \qquad a_i = [\xi_i], \qquad \xi_i = \frac{m_i + \sqrt{d}}{q_i},$$

$$m_{i+1} = a_i q_i - m_i, \qquad q_{i+1} = \frac{d - m_{i+1}^2}{q_i}$$

definen las sucesiones infinitas de los enteros $m_i$, $q_i$, $a_i$ e irracionales $\xi_i$ en tal forma que se cumplen las ecuaciones (7.7), y de donde se tendrá el desarrollo fraccionario continuado de $\xi_0$.

En primer lugar, empecemos con $\xi_0$, $m_0$, $q_0$ tal y como se determinaron anteriormente y hagamos $a_0 = [\xi_0]$. Si se conocen $\xi_i$, $m_i$, $q_i$, $a_i$, entonces se tiene $m_{i+1} = a_i q_i - m_i$, $q_{i+1} = (d - m_{i+1}^2)/q_i$, $\xi_{i+1} = (m_{i+1} + \sqrt{d})/q_{i+1}$, $a_{i+1} = [\xi_{i+1}]$. Es decir, (7.16) realmente determinan las sucesiones $\xi_i$, $m_i$, $q_i$, $a_i$ que son por lo menos reales.

Ahora se aplica la inducción matemática para probar que los $m_i$ y los $q_i$ son enteros tales que $q_i \neq 0$ y $q_i | (d - m^2)$. Esto se cumple para $i = 0$. Si es verdadero en el $i$-ésimo paso, se observa que $m_{i+1} = a_i q_i - m_i$ es un entero. Entonces la ecuación

$$q_{i+1} = \frac{d - m_{i+1}^2}{q_i} = \frac{d - m_i^2}{q_i} + 2a_i m_i - a_i^2 q_i$$

establece que $q_{i+1}$ es un entero. Es más, $q_{i+1}$ no puede ser cero, dado que si lo fuera, se tendría $d = m_{i+1}^2$, mientras que $d$ no es un cuadrado perfecto. Finalmente, se tiene $q_i = (d - m_{i+1}^2)/q_{i+1}$, de modo que $q_{i+1} | (d - m_{i+1}^2)$.

A continuación puede verificarse que

$$\xi_i - a_i = \frac{-a_i q_i + m_i + \sqrt{d}}{q_i} = \frac{\sqrt{d} - m_{i+1}}{q_i} = \frac{d - m_{i+1}^2}{q_i(\sqrt{d} + m_{i+1})}$$

$$= \frac{q_{i+1}}{\sqrt{d} + m_{i+1}} = \frac{1}{\xi_{i+1}},$$

lo cual verifica (7.7) y así se ha probado que $\xi_0 = \langle a_0, a_1, a_2, \cdots \rangle$, con los $a_i$ definidos por (7.16).

Mediante $\xi'_i$ denotemos el conjugado de $\xi_i$, esto es, $\xi'_i = (m_i - \sqrt{d})/q_i$. Dado que el conjugado de un cociente es igual al cociente de los conjugados, se obtiene la ecuación

$$\xi'_0 = \frac{\xi'_n h_{n-1} + h_{n-2}}{\xi'_n k_{n-1} + k_{n-2}}$$

tomando los conjugados en (7.8). Resolviendo para $\xi'_n$ se tiene

$$\xi'_n = -\frac{k_{n-2}}{k_{n-1}}\left(\frac{\xi'_0 - h_{n-2}/k_{n-2}}{\xi'_0 - h_{n-1}/k_{n-1}}\right).$$

Conforme $n$ tiende al infinito, tanto $h_{n-1}/k_{n-1}$ como $h_{n-2}/k_{n-2}$ tienden hacia $\xi_0$, el cual es diferente a $\xi'_0$ y por tanto la fracción que se encuentra dentro del paréntesis tiende a 1. Así que para un $n$ lo suficientemente grande, digamos $n > N$, donde $N$ es fijo, la fracción del paréntesis es positiva y $\xi'_n$ es negativo. Pero $\xi_n$ es positivo para $n \geqq 1$ y de aquí que $\xi_n - \xi'_n > 0$ para $n > N$. Aplicando (7.16) se ve que esto da $2\sqrt{d}/q_n > 0$ y de aquí que $q_n > 0$ para $n > N$.

De (7.16) también se deduce que

$$q_n q_{n+1} = d - m_{n+1}^2 \leqq d, \qquad q_n \leqq q_n q_{n+1} \leqq d$$

$$m_{n+1}^2 < m_{n+1}^2 + q_n q_{n+1} = d, \qquad |m_{n+1}| < \sqrt{d},$$

para $n > N$. Supuesto que $d$ es un entero positivo fijo se concluye que $q_n$ y $m_{n+1}$ pueden asumir sólo un número fijo de valores posibles para $n > N$. De aquí que las parejas ordenadas $(m_n, q_n)$ pueden asumir sólo un número fijo de valores posibles de las parejas para $n > N$, y por tanto existen enteros distintos $j$ y $k$ tales que $m_j = m_k$ y $q_j = q_k$. Puede suponerse que se han escogido $j$ y $k$ de manera que $j < k$. Por (7.16), esto implica que $\xi_j = \xi_k$ y de aquí que

$$\xi_0 = \langle a_0, a_1, \cdots, a_{j-1}, \overline{a_j, a_{j+1}, \cdots, a_{k-1}}\rangle.$$

La demostración del teorema 7.19 se ha completado ahora.

A continuación se determinará la subclase de irracionales cuadráticos reales que tengan desarróllos fraccionarios continuados puramente periódicos esto es, expresiones de la forma $\langle\overline{a_0, a_1, \cdots, a_n}\rangle$.

**Teorema 7.20** *El desarrollo fraccionario continuado del número irracional real $\xi$ es puramente periódico si, y solamente si, $\xi > 1$ y $-1 < \xi' < 0$, donde $\xi'$ denota el conjugado de $\xi$.*

*Demostración.* Primero se supone que $\xi > 1$ y $-1 < \xi' < 0$. Como es costumbre, se escribe $\xi_0$ por $\xi$ y se toman los conjugados en (7.7) para obtener.

(7.17) $$\frac{1}{\xi'_{i+1}} = \xi'_i - a_i.$$

Ahora bien, $a_i \geqq 1$ para todo $i$, incluso para $i = 0$, dado que $\xi_0 > 1$. De aquí que si $\xi'_i < 0$, entonces $1/\xi'_{i+1} < -1$ y se tiene $-1 < \xi'_{i+1} < 0$. Supuesto que $-1 < \xi'_0 < 0$ se ve, por inducción matemática, que $-1 < \xi'_i < 0$ se cumple para todo $i \geqq 0$. Entonces, dado que por (7.17) $\xi'_i = a_i + 1/\xi'_{i+1}$, se tiene

$$0 < -\frac{1}{\xi'_{i+1}} - a_i < 1, \qquad a_i = \left[-\frac{1}{\xi'_{i+1}}\right].$$

Ahora bien, $\xi$ es un irracional cuadrático, de modo que $\xi_j = \xi_k$ para algunos enteros $j$ y $k$ con $0 < j < k$. Entonces se tiene $\xi'_j = \xi'_k$ y

$$a_{j-1} = \left[-\frac{1}{\xi'_j}\right] = \left[-\frac{1}{\xi'_k}\right] = a_{k-1},$$

$$\xi_{j-1} = a_{j-1} + \frac{1}{\xi_j} = a_{k-1} + \frac{1}{\xi_k} = \xi_{k-1}.$$

Así que $\xi_j = \xi_k$ implica $\xi_{j-1} = \xi_{k-1}$. Una iteración de multiplicidad $j$ de esta implicación nos da $\xi_0 = \xi_{k-j}$ y se tiene

$$\xi = \xi_0 = \langle\overline{a_0, a_1, \cdots, a_{k-j-1}}\rangle.$$

Para probar la inversa, supongamos que $\xi$ es puramente periódico, digamos $\xi = \langle\overline{a_0, a_1, \cdots, a_{n-1}}\rangle$, donde $a_0, a_1, \cdots, a_{n-1}$ son enteros positivos. Entonces $\xi > a_0 \geqq 1$. También, por (7.8) se tiene

$$\xi = \langle a_0, a_1, \cdots, a_{n-1}, \xi\rangle = \frac{\xi h_{n-1} + h_{n-2}}{\xi k_{n-1} + k_{n-2}}.$$

así, $\xi$ satisface la ecuación

$$f(x) = x^2 k_{n-1} + x(k_{n-2} - h_{n-1}) - h_{n-2} = 0.$$

Esta ecuación cuadrática tiene dos raíces, $\xi$ y su conjugado $\xi'$. Supuesto que $\xi > 1$, sólo es necesario probar que $f(x)$ tiene una raíz entre $-1$ y $0$ para establecer que $-1 < \xi' < 0$. Esto se hará demostrando que $f(-1)$ y $f(0)$ tienen signos opuestos. Primero se observa que $f(0) = -h_{n-2} < 0$, por (7.6), ya que $a_i > 0$ para $i \geqq 0$. En seguida se ve que para $n > 1$

$$\begin{aligned} f(-1) &= k_{n-1} - k_{n-2} + h_{n-1} - h_{n-2} \\ &= (k_{n-2} + h_{n-2})(a_{n-1} - 1) + k_{n-3} + h_{n-3} \\ &\geqq k_{n-3} + h_{n-3} > 0. \end{aligned}$$

Finalmente, si $n = 1$, se tiene $f(-1) = k_0 - k_{-1} + h_0 - h_{-1} = a_0 > 0$, y esto completa la demostración.

Ahora enfocaremos nuestra atención al desarrollo fraccionario continuado de $\sqrt{d}$ para un entero positivo $d$ que no sea un cuadrado perfecto. Se obtiene considerando el número irracional íntimamente relacionado $\sqrt{d} + [\sqrt{d}]$. Este número satisface las condiciones del Teorema 7.20 y, por tanto, su fracción continuada es puramente periódica,

$$(7.18) \quad \sqrt{d} + [\sqrt{d}] = \langle \overline{a_0, a_1, \cdots, a_{r-1}} \rangle = \langle a_0, \overline{a_1, \cdots, a_{r-1}, a_0} \rangle.$$

Puede suponerse que se ha escogido $r$ como el menor entero para el cual $\sqrt{d} + [\sqrt{d}]$ tiene un desarrollo de la forma (7.18). Ahora se observa que $\xi_i = \langle a_i, a_{i+1} \cdots \rangle$ es puramente periódico para todos los valores de $i$, y que $\xi_0 = \xi_r = \xi_{2r} = \cdots$. Además $\xi_1, \xi_2, \cdots, \xi_{r-1}$ son todos diferentes de $\xi_0$, dado que de otra manera sería un período más corto. Así que $\xi_i = \xi_0$ si y solamente si $i$ es de la forma $mr$.

Ahora puede empezarse con $\xi_0 = \sqrt{d} + [\sqrt{d}]$, $q_0 = 1$, $m_0 = [\sqrt{d}]$ en (7.16) debido a que $1 | (d - [\sqrt{d}]^2)$. Entonces, para todo $j \geqq 0$,

$$(7.19) \quad \frac{m_{jr} + \sqrt{d}}{q_{jr}} = \xi_{jr} = \xi_0 = \frac{m_0 + \sqrt{d}}{q_0} = [\sqrt{d}] + \sqrt{d},$$

$$m_{jr} - q_{jr}[\sqrt{d}] = (q_{jr} - 1)\sqrt{d},$$

y de aquí que $q_{jr} = 1$ ya que el primer miembro es racional y $\sqrt{d}$ es irracional. Aún más, para ningún otro valor del subíndice $i$, $q_i = 1$. Porque $q_i = 1$ implica $\xi_i = m_i + \sqrt{d}$, pero $\xi_i$ tiene un desarrollo puramente periódico de modo que, por el Teorema 7.20, se tiene $-1 < m_i - \sqrt{d} < 0$, $\sqrt{d} - 1 < m_i < \sqrt{d}$ y, por tanto, $m_i = [\sqrt{d}]$. De donde $\xi_i = \xi_0$ e $i$ es un múltiplo de $r$.

También se establecerá que $q_i = -1$ no se cumple para cualquier $i$. Porque, por (7.16), $q_i = -1$ implica $\xi_i = -m_i - \sqrt{d}$, y, por el Teorema 7.20, se tendría $-m_i - \sqrt{d} > 1$ y $-1 < -m_i + \sqrt{d} < 0$. Pero esto implica $\sqrt{d} < m_i < -\sqrt{d} - 1$ lo cual es imposible.

Notando que $a_0 = [\sqrt{d} + [\sqrt{d}]] = 2[\sqrt{d}]$, ahora puede considerarse el caso $\xi = \sqrt{d}$. Aplicando (7.18) se tiene

$$\begin{aligned} \sqrt{d} &= -[\sqrt{d}] + (\sqrt{d} + [\sqrt{d}]) \\ &= -[\sqrt{d}] + \langle 2[\sqrt{d}], \overline{a_1, a_2, \cdots, a_{r-1}, a_0} \rangle \\ &= \langle [\sqrt{d}], \overline{a_1, a_2, \cdots, a_{r-1}, a_0} \rangle \end{aligned}$$

con $a_0 = 2[\sqrt{d}]$.

Cuando se aplica (7.16) a $\sqrt{d} + [\sqrt{d}]$, $q_0 = 1$, $m_0 = [\sqrt{d}]$ se tiene $a_0 = 2[\sqrt{d}]$, $m_1 = [\sqrt{d}]$, $q_1 = d - [\sqrt{d}]^2$. Pero también puede aplicarse

(7.16) a $\sqrt{d}$ con $q_0 = 1$, $m_0 = 0$ y se encuentra $a_0 = [\sqrt{d}]$, $m_1 = [\sqrt{d}]$, $q_1 = d - [\sqrt{d}]^2$. El valor de $a_0$ es diferente, pero los valores de $m_1$ y de $q_1$ son los mismos en ambos casos. Dado que $\xi_i = (m_i + \sqrt{d})/q_i$ se ve que la aplicación adicional de (7.16) proporciona los mismos valores para los $a_i$, para los $m_i$ y para los $q_i$, en ambos casos. En otras palabras, los desarrollos de $\sqrt{d} + [\sqrt{d}]$ y $\sqrt{d}$ sólo difieren en los valores de $a_0$ y $m_0$. Estableciendo los resultados explícitamente para el caso $\sqrt{d}$ se tiene el siguiente teorema.

**Teorema 7.21** *Si el entero positivo d no es un cuadrado perfecto, el desarrollo fraccionario continuado simple de $\sqrt{d}$ tiene la forma $\sqrt{d} = \langle a_0, \overline{a_1, a_2, \cdots, a_{r-1}, 2a_0} \rangle$ con $a_0 = [\sqrt{d}]$. Además, con $\xi_0 = \sqrt{d}$, $q_0 = 1$, $m_0 = 0$, en las ecuaciones (7.16), se tiene $q_i = 1$ si y solamente si $r|i$ y $q_i = -1$ se cumple para ningún subíndice i. Aquí r denota la longitud del período más corto en el desarrollo de $\sqrt{d}$.*

**Problema**

1. ¿Para qué enteros positivos $c$ el irracional cuadrático $([\sqrt{d}] + \sqrt{d})/c$ tiene un desarrollo puramente periódico?

## 7.8 Ecuación de Pell

La ecuación $x^2 - dy^2 = N$, con los enteros $d$ y $N$ dados y las incógnitas $x$ y $y$, generalmente se conoce como ecuación de Pell. Si $d$ es negativo, puede tener sólo un número finito de soluciones. Si $d$ es un cuadrado perfecto, digamos $d = a^2$, la ecuación se reduce a $(x - ay)(x + ay) = N$ y nuevamente solo existe un número finito de soluciones. El caso más interesante de la ecuación se obtiene cuando $d$ es un entero positivo que no sea un cuadrado perfecto. Para este caso son muy útiles las fracciones continuadas simples.

Se desarrolla $\sqrt{d}$ en un desarrollo fraccionario continuado como en el Teorema 7.21, con los convergentes $h_n/k_n$ y con $q_n$ definidos por las ecuaciones (7.16) con $\xi_0 = \sqrt{d}$, $q_0 = 1$, $m_0 = 0$.

**Teorema 7.22** *Si d es un entero positivo que no sea un cuadrado perfecto, entonces $h_n^2 - dk_n^2 = (-1)^{n-1} q_{n+1}$ para todos los enteros $n \geqq -1$.*

*Demostración.* A partir de las ecuaciones (7.8) y (7.16) se tiene

$$\sqrt{d} = \xi_0 = \frac{\xi_{n+1}h_n + h_{n-1}}{\xi_{n+1}k_n + k_{n-1}} = \frac{(m_{n+1} + \sqrt{d})h_n + q_{n+1}h_{n-1}}{(m_{n+1} + \sqrt{d})k_n + q_{n+1}k_{n-1}}.$$

Simplificamos esta ecuación y la separamos en un racional y una parte puramente irracional en forma muy semejante a la aplicada en (7.19). Cada parte debe ser cero, de modo que se obtienen dos ecuaciones y, a partir de ellas, puede eliminarse $m_{n+1}$. El resultado final es

$$h_n^2 - dk_n^2 = (h_n k_{n-1} - h_{n-1} k_n) q_{n+1} = (-1)^{n-1} q_{n+1},$$

donde se aplicó el Teorema 7.5 en el último paso.

**Corolario 7.23** *Tomando $r$ como la longitud del período del desarrollo de $\sqrt{d}$, como en el Teorema* 7.21, *para $n \geqq 0$ se tiene*

$$h_{nr-1}^2 - dk_{nr-1}^2 = (-1)^{nr} q_{nr} = (-1)^{nr}.$$

Puede verse que el Teorema 7.22 da las soluciones de la ecuación de Pell para ciertos valores de $N$. En particular, el Corolario 7.23 proporciona un número infinito de soluciones de $x^2 - dy^2 = 1$ mediante el uso de los valores pares $nr$. Por supuesto que si $r$ es par, todos los valores de $nr$ son pares. Si $r$ es impar, el Corolario 7.23 da un número infinito de soluciones de $x^2 - dy^2 = -1$ mediante el uso de los enteros impares $n \geqq 1$. El siguiente Teorema demuestra que toda solución de $x^2 - dy^2 = \pm 1$ puede obtenerse a partir del desarrollo fraccionario continuado de $\sqrt{d}$. Pero primero hagamos esta simple observación: aparte de las soluciones triviales tales como $x = \pm 1$, $y = 0$ de $x^2 - dy^2 = 1$, todas las soluciones de $x^2 - dy^2 = N$ caen en conjuntos de cuatro por todas las combinaciones de signos $\pm x$, $\pm y$. De aquí que es suficiente con discutir las soluciones positivas $x > 0$, $y > 0$.

**Teorema 7.24** *Sea $d$ un entero positivo que no sea un cuadrado perfecto y sean $h_n/k_n$ los convergentes para el desarrollo fraccionario continuado de $\sqrt{d}$. Supóngase que el entero $N$ satisface $|N| < \sqrt{d}$. Entonces cualquier solución positiva $x = s$, $y = t$ de $x^2 - dy^2 = N$ con $(s, t) = 1$ satisface $s = h_n$, $t = k_n$ para algún entero positivo $n$.*

*Demostración.* Sean $E$ y $M$ enteros positivos tales que $(E, M) = 1$ y $E^2 - \rho M^2 = \sigma$, donde $\sqrt{\rho}$ es irracional y $0 < \sigma < \sqrt{\rho}$. Aquí $\rho$ y $\sigma$ son números reales, no necesariamente enteros. Entonces

$$\frac{E}{M} - \sqrt{\rho} = \frac{\sigma}{M(E + M\sqrt{\rho})},$$

y de aquí que

$$0 < \frac{E}{M} - \sqrt{\rho} < \frac{\sqrt{\rho}}{M(E + M\sqrt{\rho})} = \frac{1}{M^2(E/(M\sqrt{\rho}) + 1)}.$$

También $0 < E/M - \sqrt{\rho}$ implica $E/M\sqrt{\rho}) > 1$ y, por lo tanto,

$$\left|\frac{E}{M} - \sqrt{\rho}\right| < \frac{1}{2M^2}.$$

Por el Teorema 7.14, $E/M$ es un convergente en el desarrollo fraccionario continuado de $\sqrt{\rho}$.

Si $N > 0$, se toma $\sigma = N$, $\rho = d$, $E = s$, $M = t$ y el teorema se cumple en este caso.

Si $N < 0$, entonces $t^2 - (1/d)s^2 = -N/d$ y se toma $\sigma = -N/d$, $\rho = 1/d$, $E = t$, $M = s$. Se encuentra que $t/s$ es un convergente en el desarrollo de $1/\sqrt{d}$. Entonces el Teorema 7.15 demuestra que $s/t$ es un convergente en el desarrollo de $\sqrt{d}$.

**Teorema 7.25** *Todas las soluciones positivas de* $x^2 - dy^2 = \pm 1$ *se encuentran entre* $x = h_n$, $y = k_n$, *donde* $h_n/k_n$ *son los convergentes del desarrollo de* $\sqrt{d}$. *Si* $r$ *es el período del desarrollo de* $\sqrt{d}$, *como en el Teorema* 7.21, *y si* $r$ *es par entonces* $x^2 - dy^2 = -1$ *no tiene soluciones y todas las soluciones positivas de* $x^2 - dy^2 = 1$ *están dadas por* $x = h_{nr-1}$, $y = k_{nr-1}$ *para* $n = 1, 2, 3, \cdots$. *Por otra parte, si* $r$ *es impar, entonces* $x = h_{nr-1}$, $y = k_{nr-1}$ *dan todas las soluciones positivas de* $x^2 - dy^2 = -1$ *mediante el uso de* $n = 1, 3, 5, \cdots$, *y todas las soluciones positivas de* $x^2 - dy^2 = 1$ *mediante el uso de* $n = 2, 4, 6, \cdots$.

*Demostración.* Este resultado es un corolario de los Teoremas 7.21, 7.22 y 7.24.

La sucesión de pares $(h_0, k_0)$, $(h_1, k_1)$, $\cdots$ incluirán todas las soluciones positivas de $x^2 - dy^2 = 1$. Además, $a_0 = [\sqrt{d}] > 0$ de manera que la sucesión $h_0, h_1, h_2, \cdots$ es estrictamente creciente. Si se denota por $x_1$, $y_1$ la primera solución que aparece, entonces para toda otra solución $x$, $y$ se tendrá $x > x_1$ y, de donde, también $y > y_1$. Habiendo encontrado esta menor solución positiva por medio de las fracciones continuadas, pueden encontrarse todas las demás soluciones positivas mediante un método más sencillo.

**Teorema 7.26** *Sea* $x_1, y_1$ *la menor solución positiva de* $x^2 - dy^2 = 1$, *siendo* $d$ *un entero positivo que no es un cuadrado perfecto. Entonces todas las soluciones positivas están dadas por* $x_n, y_n$ *para* $n = 1, 2, 3, \cdots$ *donde* $x_n$ *y* $y_n$ *son los enteros definidos por* $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$.

Los valores de $x_n$ y $y_n$ se determinan desarrollandc la potencia e igualando las partes racionales y las partes puramente irracionales. Por ejemplo, $x_3 + y_3\sqrt{d} = (x_1 + y_1\sqrt{d})^3$ de manera que $x_3 = x_1^3 + 3x_1y_1^2d$ y $y_3 = 3x_1^2y_1 + y_1^3d$.

*Demostración.* Primero se establece que $x_n$, $y_n$ es una solución. Se tiene $x_n - y_n\sqrt{d} = (x_1 - y_1\sqrt{d})^n$, dado que el conjugado de un producto es el producto de los conjugados. De aquí que puede escribirse.

$$x_n^2 - y_n^2 d = (x_n - y_n \sqrt{d})(x_n + y_n \sqrt{d})$$
$$= (x_1 - y_1 \sqrt{d})^n (x_1 + y_1 \sqrt{d})^n = (x_1^2 - y_1^2 d)^n = 1.$$

En seguida se demuestra que puede obtenerse toda solución positiva. Supóngase que se tiene una solución positiva $s$, $t$ que no se encuentra en la colección $\{x_n, y_n\}$. Dado que tanto $x_1 + y_1 \sqrt{d}$ como $s + t \sqrt{d}$ son mayores que 1, debe existir algún entero $m$ tal que $(x_1 + y_1 \sqrt{d})^m \leqq s + t \sqrt{d} < (x_1 + y_1 \sqrt{d})^{m+1}$. No puede tenerse $(x_1 + y_1 \sqrt{d})^m = s + t \sqrt{d}$ porque esto implicaría $x_m + y_m \sqrt{d} = s + t\sqrt{d}$ y de donde $s = x_m$, $t = y_m$. Ahora bien, $(x_1 - y_1 \sqrt{d})^m = (x_1 + y_1 \sqrt{d})^{-m}$ y puede multiplicarse la desigualdad anterior por $(x_1 - y_1 \sqrt{d})^m$ para obtener $1 < (s + t \sqrt{d})(x_1 - y_1 \sqrt{d})^m < x_1 + y_1 \sqrt{d}$.

Definiendo los enteros $a$ y $b$ por $a + b \sqrt{d} = (s + t \sqrt{d})(x_1 - y_1 \sqrt{d})^m$ se tiene

$$a^2 - b^2 d = (s^2 - t^2 d)(x_1^2 - y_1^2 d)^m = 1$$

de manera que $a$, $b$ es una solución de $x^2 - dy^2 = 1$ tal que $1 < a + b \sqrt{d} < x_1 + y_1 \sqrt{d}$. Pero entonces $0 < (a + b \sqrt{d})^{-1} < 1$ y, por tanto, $0 < a - b \sqrt{d} < 1$. Ahora se tiene

$$a = \tfrac{1}{2}(a + b \sqrt{d}) + \tfrac{1}{2}(a - b \sqrt{d}) > \tfrac{1}{2} + 0 > 0,$$

$$b \sqrt{d} = \tfrac{1}{2}(a + b \sqrt{d}) - \tfrac{1}{2}(a - b \sqrt{d}) > \tfrac{1}{2} - \tfrac{1}{2} = 0,$$

de manera que $a$, $b$ es una solución positiva. Por tanto, $a > x_1$, $b > y_1$, pero esto contradice $a + b \sqrt{d} < x_1 + y_1 \sqrt{d}$ y de aquí que nuestra suposición fue falsa. Todas las soluciones positivas están dadas por $x_n$, $y_n$, $n = 1, 2, 3, \ldots$.

Puede observarse que la definición de $x_n$, $y_n$ puede extenderse para $n$ cero y negativo. Entonces dan soluciones no positivas.

Para $N$ diferente de 1 existen ciertos resultados que pueden probarse, pero no están tan completos como lo que se ha demostrado que es cierto en el caso $N = 1$. Por ejemplo, si $x_1$, $y_1$ es la solución positiva menor de $x^2 - dy^2 = 1$ y si $r_0^2 - ds_0^2 = N$, entonces pueden definirse los enteros $r_n$, $s_n$ por $r_n + s_n \sqrt{d} = (r_0 + s_0 \sqrt{d})(x_1 + y_1 \sqrt{d})^n$ y es fácil demostrar que $r_n$, $s_n$ son soluciones de $x^2 - dy^2 = N$. Sin embargo, no hay seguridad de que todas las soluciones positivas puedan obtenerse en esta forma partiendo de una $r_0$, $s_0$, fija.

**Problemas**

El símbolo $d$ denota un entero positivo, no cuadrado perfecto.

1. Suponiendo que $x^2 - dy^2 = -1$ tiene solución, sea $x_1$, $y_1$ la menor solución positiva. Probar que $x_2$, $y_2$, definida por $x_2 + y_2\sqrt{d} = (x_1 + y_1\sqrt{d})^2$ es la solución positiva menor de $x^2 - dy^2 = -1$. Probar también que todas las soluciones de $x^2 - dy^2 = -1$ están dadas por $x_n$, $y_n$, donde $x_n + y_n\sqrt{d} = (x_1 + y_1\sqrt{d})^n$, con $n = 1, 3, 5, 7, \cdots$, y que todas las soluciones de $x^2 - dy^2 = 1$ están dadas por $x_n$, $y_n$ con $n = 2, 4, 6, 8, \cdots$.
2. Probar que si $x^2 - dy^2 = N$ tiene una solución, tiene un número infinito. *Sugerencia*: usar la identidad $(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 - dy_1y_2)^2 - d(x_1y_2 - x_2y_1)^2$.
3. Probar que $x^2 - dy^2 = -1$ no tiene solución si $d \equiv 3 \pmod 4$.
4. Sea $d$ un entero positivo, no cuadrado perfecto. Si $k$ es cualquier entero positivo, probar que existe un número infinito de soluciones en los enteros de $x^2 - dy^2 = 1$ con $k|y$.

## 7.9 Cálculo numérico

Los cálculos numéricos relacionados con la búsqueda de una fracción continuada simple pueden ser más bien largos. En general, debe aplicarse el algoritmo (7.7). No obstante, si $\xi_0$ es un irracional cuadrático puede simplificarse el trabajo. Probablemente sea mejor aplicar (7.16) en una forma ligeramente alterada. De (7.16) se tiene

$$q_{i+1} = \frac{d - m_{i+1}^2}{q_i} = \frac{d - (a_iq_i - m_i)^2}{q_i} = \frac{d - m_i^2}{q_i} - a_i^2q_i + 2a_im_i$$
$$= q_{i-1} - a_i(a_iq_i - m_i) + a_im_i = q_{i-1} + a_i(m_i - m_{i+1}).$$

Partiendo con $\xi_0 = (m_0 + \sqrt{d})/q_0$, $q_0|(d - m_0^2)$ se obtiene, a su vez

$$a_0 = \left[\frac{m_0 + \sqrt{d}}{q_0}\right], \quad m_1 = a_0q_0 - m_0, \quad q_1 = \frac{d - m_1^2}{q_0},$$

$$a_1 = \left[\frac{m_1 + \sqrt{d}}{q_1}\right], \quad m_2 = a_1q_1 - m_1, \quad q_2 = q_0 + a_1(m_1 - m_2),$$

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

$$a_{i-1} = \left[\frac{m_{i-1} + \sqrt{d}}{q_{i-1}}\right], \quad m_i = a_{i-1}q_{i-1} - m_{i-1},$$
$$q_i = q_{i-2} + a_{i-1}(m_{i-1} - m_i), \qquad i \geqq 1.$$

La fórmula $q_iq_{i+1} = d - m_{i+1}^2$ sirve como una buena comprobación. Incluso para números grandes, este procedimiento es medianamente sencillo para llevarlo a cabo.

Para números más bien pequeños frecuentemente es más fácil obtener directamente el desarrollo. Por ejemplo, para $\sqrt{3}$ puede calcularse del modo siguiente:

$$\xi_0 = \sqrt{3} = 1 + \frac{1}{\xi_1},$$

$$\xi_1 = \frac{1}{\sqrt{3} - 1} = \frac{\sqrt{3} + 1}{2} = 1 + \frac{1}{\xi_2},$$

$$\xi_2 = \frac{2}{\sqrt{3} - 1} = \sqrt{3} + 1 = 2 + \frac{1}{\xi_3},$$

$$\xi_3 = \frac{1}{\sqrt{3} - 1}.$$

En este caso $\xi_3 = \xi_1$ y, en tal caso, ahí termina. Se tiene

$$a_0 = 1, \; a_1 = 1, \; a_2 = 2, \; a_3 = a_1 = 1, \; \ldots, \; \sqrt{3} = \langle 1, \overline{1, 2} \rangle.$$

Cuando se conoce una fracción continuada pueden obtenerse los convergentes de (7.6). El trabajo puede sistematizarse. El ejemplo siguiente, para $\sqrt{3}$ demuestra un método más conveniente.

| | | |
|---|---|---|
| | 0 | 1 |
| | 1 | 0 |
| 1 | 1 | 1 |
| 1 | 2 | 1 |
| 2 | 5 | 3 |
| 1 | 7 | 4 |
| 2 | 19 | 11 |
| . | . | . |
| . | . | . |
| . | . | . |

$h_0 = 1, k_0 = 1$

$h_1 = 2, k_1 = 1$

$h_2 = 5, k_2 = 3$

. . . . . . . . . .

# Capítulo 8

# Observaciones elementales sobre la distribución de los primos

## 8.1 La función $\pi(x)$

La discusión de la Sección 1.3 evidencia que los primos estan distribuidos entre los números naturales de una manera muy irregular. El Teorema 1.18 demuestra que existen arbitrariamente grandes saltos en la sucesión de los primos. La prueba del Teorema 1.17 no solamente muestra que existe un número infinito de primos sino que también el $r$-ésimo primo $p_r$ no es mayor que $\prod_{j=1}^{r-1} p_j + 1$, el producto de los $r - 1$ primeros primos más 1. Un pequeño cambio en la demostración muestra que $p_r \leqq \prod_{j=1}^{r-1} p_j - 1$ si $r > 2$.

En este capítulo abandonaremos nuestra convención de que las letras del alfabeto romano representan enteros.

**Definición 8.1** *Para un $x$ real, denotemos por $\pi(x)$ el número de primos que no excedan a $x$. Así por ejemplo*

$$\pi(-1) = \pi(1) = 0, \qquad \pi(2) = \pi(5/2) = 1.$$

**Teorema 8.1** *Existen las constantes positivas $a$ y $b$ tales que*

$$a\frac{x}{\log x} < \pi(x) < b\frac{x}{\log x}$$

*para* $x \geqq 2$.

*Demostración.* Para un entero positivo $n$ y un primo $p$ sea $p^{\mu_p}$ la mayor potencia de $p$ que divide al coeficiente binominal $\binom{2n}{n}$. De acuerdo con el Teorema 4.2

(8.1) $$\mu_p = \sum_{j\geqq 1}\left(\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right]\right).$$

Definamos el entero $\nu_p$ mediante las desigualdades $p^{\nu_p} \leqq p^{1+\nu_p}$. Evidentemente $\nu_p$ existe y es único. Entonces $\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right] = 0 - 0 = 0$ para $j > \nu_p$. También para todo $j$, se tiene

$$\left[\frac{2n}{p^j}\right] - 2\left[\frac{n}{p^j}\right] < \frac{2n}{p^j} - 2\left(\frac{n}{p^j} - 1\right) = 2$$

y de aquí que $[2n/p^j] - 2[n/p^j] \leqq 1$ para todo $j \geqq 1$. Aplicando esto en (8.1) se obtiene

(8.2) $$\mu_p \leqq \sum_{j=1}^{\nu_p} 1 = \nu_p$$

y por tanto

(8.3) $$\binom{2n}{n} \Bigg| \prod_{p\leqq 2n} p^{\nu_p}.$$

Por otra parte, si $n < p \leqq 2n$, entonces $p|(2n)!$ y $p \nmid n!$ de donde se tiene $\prod_{n<p\leqq 2n} p \,\Big|\, \binom{2n}{n}$, lo cual, junto con (8.3), nos da

$$\prod_{n<p\leqq 2n} p \leqq \binom{2n}{n} \leqq \prod_{p\leqq 2n} p^{\nu_p} \leqq \prod_{p\leqq 2n} 2n$$

y de aquí, cambiando a $n$ cada $p$ en el primer producto,

(8.4) $$n^{\pi(2n)-\pi(n)} \leqq \binom{2n}{n} \leqq (2n)^{\pi(2n)}.$$

Pero $\binom{2n}{n} \leqq (1 + 1)^{2n} = 2^{2n}$ y

$$\binom{2n}{n} = \frac{(2n)(2n-1)\cdots(n+1)}{n!} = \prod_{j=1}^{n} \frac{n+j}{j} \geqq \prod_{j=1}^{n} 2 = 2^n.$$

Aplicando estas desigualdades en (8.4) y tomando logaritmos se obtiene

(8.5) $$\pi(2n) - \pi(n) \leqq \frac{2n \log 2}{\log n}, \qquad \pi(2n) \geqq \frac{n \log 2}{\log (2n)}$$

donde debe suponerse que, en la primera igualdad, $n > 1$.

Para todo real $x \geqq 2$, supóngase que $2n$ es el mayor entero par que no excede a $x$. Entonces se tiene $x \geqq 2n$, $n \geqq 1$, $2n > x$ y, de donde,

$$\pi(x) \geqq \pi(2n) \geqq \frac{n \log 2}{\log (2n)} \geqq \frac{n \log 2}{\log x} \geqq \frac{(2n+2)\log 2}{4 \log x} > \frac{\log 2}{4}\,\frac{x}{\log x}$$

Para obtener la otra mitad de la desigualdad se aplica la primera parte de (8.5). Para todo real $y \geqq 4$, supóngase que $2n$ es el menor entero par no menor que $y$. Se tiene $y \leqq 2n$, $\pi(y) \leqq \pi(2n)$, $y + 2 > 2n$, $\frac{y}{2} > n - 1$, $\pi\left(\frac{y}{2}\right) \geqq \pi(n-1) \geqq \pi(n) - 1$, y de aquí que

$$\pi(y) - \pi\left(\frac{y}{2}\right) \leqq \pi(2n) - \pi(n) + 1 \leqq \frac{2n \log 2}{\log n} + 1 \leqq \frac{(y+2)\log 2}{\log (y/2)} + 1$$

$$\leqq \frac{2(y+2)\log 2}{\log y} + 1 \leqq \frac{3y \log 2}{\log y} + 1 < \frac{4y \log 2}{\log y}.$$

Por lo tanto $\pi(y) - \pi(y/2) < (4 \log 2) y/\log y$ si $y \geqq 4$. Pero, para $2 \leqq y < 4$ se tiene $\pi(y) - \pi(y/2) \leqq \pi(4) = 2$ y fácilmente se ve que la función $y/\log y$ toma su valor mínimo, $e$, cuando $y = e$. De donde se tiene

$$\pi(y) - \pi\left(\frac{y}{2}\right) \leqq \frac{(2/e)y}{\log y} \quad \text{para } 2 \leqq y < 4,$$

y de aquí que

$$\pi(y) - \pi\left(\frac{y}{2}\right) < \frac{(4 \log 2)y}{\log y} \quad \text{para } y \geqq 2$$

dado que $2/e < 4 \log 2$. Ahora bien, para $y \geqq 2$ se tiene

$$\text{(8.6)} \quad \pi(y) \log y - \pi\left(\frac{y}{2}\right) \log \frac{y}{2} = \left(\pi(y) - \pi\left(\frac{y}{2}\right)\right) \log y$$

$$+ \pi\left(\frac{y}{2}\right) \log 2 < 4y \log 2 + \frac{y}{2} \log 2 = \frac{9}{2} y \log 2.$$

Ahora, para todo real $x \geqq 2$ existe un entero no negativo $j$ tal que $2^{j+2} > x \geqq 2^{j+1}$. Se reemplaza $y$ en (8.6) por $x, x/2, x/2^2, \ldots, x/2^j$, y se suma. Dado que $x/2^{j+1} < 2$, $\pi(x/2^{j+1}) = 0$, se obtiene

$$\pi(x) \log x < \frac{9}{2}\left(x + \frac{x}{2} + \cdots + \frac{x}{2^j}\right) \log 2 < 9x \log 2.$$

Por tanto, puede tomarse $a = (\log 2)/4$, $b = \log 2$ y el teorema queda demostrado. Se han encontrado valores de $a$ y $b$ que son suficientes pero que, por ningún medio, son los mejores valores posibles.

El teorema que acaba de demostrarse dice algo acerca de que tan numerosa y escasamente están distribuidos los primos. Dado que hay un número infinito de primos, no puede decirse que hay más números naturales que primos. No obstante, la razón $\pi(n)/n$ representa la proporción de primos en los primeros $n$ números naturales. Puesto que $\pi(n)/n < b/\log n$ tiende hacia cero conforme $n$ crece, nos conduce a decir que los

primos son más escasos que los números naturales. Con frecuencia esto se establece diciendo: "casi todos los enteros positivos son compuestos". Por supuesto, el teorema dice bastante más. Dado que

$$a < \frac{\pi(x)}{x/\log x} < b,$$

la función $\pi(x)$ es de orden $x/\log x$. Los primos no son demasiado numerosos ni demasiado escasos. Puesto que

$$\frac{\sqrt{x}}{\pi(x)} < \frac{\log x}{a\sqrt{x}} \to 0 \quad \text{conforme} \quad x \to \infty,$$

la sucesión de cuadrados es más escasa que la sucesión de primos. El teorema de los números primos mencionado en la sección 1.3 es un refinamiento del presente teorema.

**Problema**

1. Probar que $v_p$, tal y como se define en relación con (8.1), es igual a $\left[\frac{\log 2n}{\log p}\right]$.

## 8.2 La sucesión de primos

Los resultados referentes a la magnitud del $r$-ésimo primo, $p_r$, también pueden usarse para describir qué tan numerosos son los primos. Nuestro primer resultado es esencialmente un corolario al teorema 8.1.

**Teorema 8.2** *Existen las constantes positivas $c$ y $d$ tales que $cr \log r < p_r < dr \log r$ para $r \geqq 2$.*

*Demostración.* Aplicando el teorema 8.1 y el hecho de que $p_r \geqq r$ se tiene

$$r = \pi(p_r) < b\frac{p_r}{\log p_r}, \qquad p_r > \frac{r \log p_r}{b} \geqq \frac{1}{b} r \log r.$$

Asimismo, se tiene $r = \pi(p) > ap_r/\log p_r$. Si $r$ es grande, también lo es $p_r$, y existe una constante $k$ tal que $\log p_r/\sqrt{p_r} < a$ si $r \geqq k$. Entonces, para $r \geqq k$,

$$r\frac{\log p_r}{p_r} > a > \frac{\log p_r}{\sqrt{p_r}}$$

de aquí que $r > \sqrt{p_r}$, $\log p_r < 2 \log r$ y por lo tanto $ap_r < r \log p_r < 2r \log r$. Si $d$ es mayor que el número mayor entre

$$\frac{2}{a}, \quad \frac{p_2}{2\log 2}, \quad \frac{p_3}{3\log 3}, \ldots, \frac{p_{k-1}}{(k-1)\log(k-1)},$$

entonces $p_r < dr \log r$ para $r \geqq 2$.

**Teorema 8.3** *La serie* $\sum_{r=1}^{\infty} \frac{1}{p_r}$ diverge.

*Demostración.* Para $r > 1$ se tiene

$$\frac{1}{p_r} > \frac{1}{dr \log r}$$

la serie $\sum_{r=2}^{\infty} 1/(r \log r)$ diverge

Si una serie $\sum_{r=1}^{\infty} a^k$ de términos positivos converge para todos los valores de $k > f$ y diverge para todos los valores de $k < f$, siendo $f$ fijo, entonces $f$ se llama el exponente de convergencia de la sucesión $a_r$. La sucesión $1/p_r$ tiene exponente de convergencia 1. Si $k > 1$, entonces $1/p^k < 1/r^k$ y $\sum_{r=1}^{\infty} 1/r^k$ converge. Si $0 < k \leqq 1$, del teorema 8.3 se deduce que $\sum_{r=1}^{\infty} 1/p_r^k$ diverge.

La sucesión $a_r = 1/r^2$ tiene exponente de convergencia $\frac{1}{2}$. En efecto, si $a_r = 1/[1^{1+\varepsilon}]$, $\varepsilon > 0$, entonces $a_r < 1/(r^{1+\varepsilon} - 1) < 2/r^{1+\varepsilon}$ si $r \geqq 2$ y la sucesión $a_r$ tiene exponente de convergencia $(1 + \varepsilon)^{-1} < 1$. En cierto sentido, los primos son más densos que la sucesión que consiste de $[r^{1+\varepsilon}]$.

**Teorema 8.4** *Existe una constante k tal que*

$$\sum_{2<p\leqq x} \frac{1}{p} < k \log\log x \qquad \text{si } x \geqq 3.$$

*Demostración.* Por el teorema 8.2

$$\sum_{2<p\leqq x} \frac{1}{p} < \sum_{r=2}^{\pi(x)} \frac{1}{cr\log r} \leqq \frac{1}{c}\sum_{r=2}^{[x]} \frac{1}{r\log r} = \frac{1}{c}\left(\frac{1}{2\log 2} + \sum_{r=3}^{[x]} \int_{r-1}^{r} \frac{dt}{r\log r}\right)$$

$$\leqq \frac{1}{2c\log 2} + \frac{1}{c}\sum_{r=3}^{[x]} \int_{r-1}^{r} \frac{dt}{t\log t} \leqq \frac{1}{2c\log 2} + \frac{1}{c}\int_{2}^{x} \frac{dt}{t\log t}$$

$$= \frac{1}{2c\log 2} + \frac{1}{c}\log\log x - \frac{1}{c}\log\log 2,$$

y esto es menor que $k \log \log x$ para $x \geqq 3$, si $k$ es lo suficientemente grande.

El método aplicado en esta demostración se presenta frecuentemente en la teoría de los números. Es el método encontrado generalmente en las demostraciones de la prueba de la integral en la teoría de las series. Para una función monótona $f(x)$, se compara $\sum_{n=M}^{N} f(n)$ con $\int_{M-1}^{N} f(x)\,dx$. Geométricamente, $\int_{M-1}^{N} f(x)\,dx$ es el área bajo la curva $y = f(x)$, mientras que $\sum_{n=M}^{N} f(n)$ representa el área cubierta por los rectángulos que tienen bases unitarias y alturas $f(n)$, $n = M, M+1, \ldots, N$.

En contraste con el teorema 8.3, el teorema 8.4 demuestra que los primos no son demasiado numerosos.

**Teorema 8.5** *Si* $x \geqq 2$ entonces $\prod_{p \leqq x} p < 4^x$

*Demostración.* Este teorema obviamente es verdadero para $2 \leqq x < 3$. Si es verdadero cuando $x$ es un entero impar $n \geqq 3$, entonces es verdadero para $n \leqq x < n+2$ dado que $\prod_{p \leqq x} p = \prod_{p \leqq n} p < 4^n < 4^x$. Por lo tanto es necesario considerar solamente los enteros impares $n$ con $n \geqq 3$. La demostración ahora es por inducción sobre el entero impar $n$. Notando que el teorema se cumple para $n = 3$, se supone el resultado para todos los enteros impares mayores que 1 que sean menores que algún entero impar $n \geqq 5$. Se define $k = (n \pm 1)/2$ donde el signo se escoge de manera que $k$ sea impar. Entonces $k \geqq 3$. Ahora bien,

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{8.7}$$

y $n - k$ es par y $n - k = 2k \mp 1 - k \leqq k + 1$. Si $p$ es un primo tal que $k < p \leqq n$ entonces $p$ es impar y $p|n!$, $p \nmid k!$, $p \nmid (n-k)!$. De aquí que de (8.7) se ve que el producto de todos esos primos divide a $\binom{n}{k}$, y así que

$$\prod_{k<p\leqq n} p \leqq \binom{n}{k}.$$

Pero $\binom{n}{k} = \binom{n}{n-k}$ y ambos de estos coeficientes binomiales aparecen en el desarrollo de $(1+1)^n$. Esto implica que $\binom{n}{k} < 2^{n-1}$. Aplicando esto y la hipótesis de inducción se tiene

$$\prod_{p\leqq n} p = \prod_{p\leqq k} p \cdot \prod_{k<p\leqq n} p < 4^k \cdot 2^{n-1} = 2^{n+2k-1} \leqq 2^{2n} = 4^n$$

debido a que $n \geqq 2k - 1$.

**Problemas**

1. Encontrar el exponente de convergencia de la sucesión de recíprocos de los enteros positivos crecientes que carecen del dígito 9 cuando se escriben en notación decimal ordinaria.
2. Dar una demostración independiente del teorema 1.18 ("Existen vacíos arbitrariamente grandes en la serie de los primos") mediante la aplicación del teorema 8.2.
3. Escribir $s_r$ para la suma de los $r$ primeros primos. Probar que existen las constantes positivas $a_1$ y $b_1$ tales que

$$a_1 r^2 \log r < s_r < b_1 r^2 \log r.$$

4. *a*) Sean $\{a_j\}$, $\{b_j\}$, $\{c_j\}$ sucesiones crecientes de números reales, cada una con límite infinito. Se dice que $a_j$ es asintótica a $b_j$, y que se escribe $a_j \sim b_j$, si y sólo si $\lim a_j/b_j = 1$. Probar que $a_j \sim b_j$ implica que $\log a_j \sim \log b_j$, pero que la inversa es falsa.
   *b*) Si $a_j \sim b_j$ probar que $b_j \sim a_j$; si $a_j \sim b_j$ y $c_j \sim d_j$ probar que $a_j c_j \sim b_j d_j$.
   *c*) Probar que $\lim (\log a_j)/a_j = 0$.
   *d*) Si $\lim c_j/a_j = 0$, probar que $a_j \sim b_j$ si y solamente si $a_j \sim b_j + c_j$.
   *e*) El teorema de los números primos establece que $\pi(n) \sim n/\log n$. Ahora se da un esquema de que esto es consecuencia de $p_n \sim n \log n$. Verificar los pasos en esta demostración y probar el resultado inverso. Nótese que $p_{n+1} \sim (n+1)\log(n+1) \sim n \log n \sim p_n$. Para los enteros $k > 1$ definir $n$ por $p_n \leqq k < p_{n+1}$, de manera que $n$ es una función de $k$ y $k \sim p_n$. También $n = \pi(k)$ y de aquí que $k \sim n \log n = \pi(k) \log \pi(k)$ y $\log k \sim \log \pi(k) + \log \log \pi(k) \sim \log \pi(k)$. Se deduce que $k \sim \pi(k) \log k$ o bien $\pi(k) \sim k/\log k$.

## 8.3 Postulado de Bertrand

**Teorema 8.6** *Para todo entero positivo $n$ existe un primo $p$ tal que $n < p \leqq 2n$.*

*Demostración.* Es sencillo comprobar que el teorema es verdadero para $n \leqq 7$. Supóngase que el resultado es falso para algún entero $n \geqq 8$. Por la definición de $\mu_p$ y (8.2), con esta suposición se tiene

$$(8.8) \qquad \binom{2n}{n} = \prod_{p \leqq 2n} p^{\mu_p} = \prod_{p \leqq n} p^{\mu_p}, \qquad \mu_p \leqq \nu_p.$$

Para todo primo $p$ en el intervalo $2n/3 < p \leqq n$ se tiene

$$p \geqq 3, \quad p^2 > \frac{2}{3} np \geqq 2n, \qquad 1 \leqq \frac{n}{p} < \frac{3}{2}, \quad 2 \leqq \frac{2n}{p} < 3$$

y así, por (8.1)

$$\mu_p = \left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 2 - 2 = 0.$$

Para todo primo $p$ en el intervalo $\sqrt{2n} < p \leqq 2n/3$ se tiene $p^2 > 2n$ y de donde $\nu_p = 1$ y $\mu_p \leqq 1$. Para todo primo $p$ que satisface $p \leqq \sqrt{2n}$ se tiene $p^{\mu_p} \leqq p^{\nu_p} \leqq 2n$. Aplicando estos hechos en (8.8) se obtiene

$$\binom{2n}{n} = \prod_{p \leqq \sqrt{2n}} p^{\mu_p} \prod_{\sqrt{2n} < p \leqq 2n/3} p^{\mu_p} \prod_{2n/3 < p \leqq n} p^{\mu_p}$$

$$\leqq \prod_{p \leqq \sqrt{2n}} 2n \prod_{p \leqq 2n/3} p.$$

El primer producto en la última expresión tiene cuando más $\sqrt{2n} - 2$ factores, dado que $\sqrt{2n} \geqq 4$ y 1 y 4 no son primos. Se aplica el Teorema 8.5 al segundo producto y entonces se tiene

$$\binom{2n}{n} \leqq (2n)^{\sqrt{2n}-2} 4^{2n/3}. \tag{8.9}$$

Ahora, $\binom{2n}{n}$ es el mayor de los $2n + 1$ términos en el desarrollo binomial de $(1 + 1)^{2n}$ de modo que se tiene

$$(2n + 1)\binom{2n}{n} > 2^{2n}.$$

Pero $4n^2 > 2n + 1$ y de aquí que

$$4n^2\binom{2n}{n} > 2^{2n}, \qquad \binom{2n}{n} > 2^{2n}(2n)^{-2}.$$

Esto con (8.9) implica que

$$2^{2n}(2n)^{-2} < (2n)^{\sqrt{2n}-2} 4^{2n/3}, \qquad 2^{2n/3} < (2n)^{\sqrt{2n}}.$$

Tomando logaritmos y dividiendo entonces entre $\sqrt{2n}$ se obtiene

$$\frac{1}{3}\sqrt{2n}\log 2 < \log(2n). \tag{8.10}$$

Pero $(1/3)\sqrt{2n}\log 2 - \log(2n)$ es positivo si $n = 405$ y

$$\frac{d}{dn}\left(\frac{1}{3}\sqrt{2n}\log 2 - \log(2n)\right) = \frac{\log 2}{3\sqrt{2n}} - \frac{1}{n},$$

lo cual es positivo para $n \geqq 38$. De aquí que (8.10) es falsa para $n \geqq 450$ y el teorema se cumple para $n \geqq 450$.

Para completar la demostración simplemente debe presentarse un $p$ apropiado para $n = 8, 9, \ldots, 449$. Puede usarse

$$\begin{array}{rlr} p = & 13 \text{ para} & 8 \leqq n \leqq 12 \\ & 23 & 13 \leqq n \leqq 22 \\ & 43 & 23 \leqq n \leqq 42 \\ & 83 & 43 \leqq n \leqq 82 \\ & 163 & 83 \leqq n \leqq 162 \\ & 317 & 163 \leqq n \leqq 316 \\ & 631 & 317 \leqq n \leqq 449 \end{array}$$

El lector puede descubrir que $n = 450$ no es el menor valor de $n$ que hace falsa a (8.10). Ese valor particular es uno fácil para sustituirlo en (8.10). Es mucho más fácil extender la tabla anterior más adelante de lo necesario que calcular valores adicionales de (8.10). De hecho la tabla como es nos llevará hasta $n = 630$.

Esta demostración es representativa de muchas demostraciones en la teoría de los números. En la demostración se usan desigualdades y se estiman las magnitudes de varias expresiones. Con frecuencia estas estimaciones son lo suficientemente buenas para probar el teorema para grandes valores de $n$, digamos, pero son demasiado toscas para proporcionar el resultado deseado para $n$ menores. Entonces es imprescindible tomar en cuenta estos $n$ menores mediante métodos más especiales.

**Problemas**

1. Probar que para todo número real positivo $x > 1$ existe un primo $p$ tal que $x < p < 2x$.
2. Probar que $n! = m^k$ es imposible en los enteros $m$, $n > 1$, $k > 1$.
3. Sean $k$ y $r$ enteros positivos, $k > 1$, $r > 1$. Probar que existe un primo cuya representación digital para la base $r$ tiene exactamente $k$ dígitos.
4. Para este problema incluir 1 como un primo. Probar que todo entero positivo puede representarse como una suma de uno o más primos distintos.
5. Probar que las siguientes tres propiedades de un entero positivo $n$ son equivalentes: (i) todos los primos $\leqq \sqrt{n}$ son divisores de $n$; (ii) todos los enteros positivos $< n$ y primos para $n$ son primos; (iii) todo entero compuesto $< n$ tiene un factor en común con $n$. Además, probar que sólo un número finito de enteros positivos tienen estas propiedades y encontrarlos. *Sugerencia:* si $n$ es lo suficientemente grande existen los primos distintos $p_1$, $p_2$, $p_3$, $p_4$ tales que $\frac{\sqrt{n}}{2^j} < p_j < \frac{\sqrt{n}}{2^{j-1}}$ para $j = 1, 2, 3, 4$.

# Capítulo 9

# Números algebraicos

## 9.1 Polinomios

Los números algebraicos son las raíces de ciertos tipos de polinomios, por tanto, es natural empezar nuestra discusión con este tópico. Nuestro plan en este capítulo es proceder desde los resultados más generales, acerca de los números algebraicos hasta los resultados específicos más fuertes en relación con las clases especiales de números algebraicos. En este proceso de probar más y más respecto a menos y menos, se ha seleccionado material de un aspecto teórico de los números en contraste con las partes más "algebraicas" de la teoría. En otras palabras, estamos interesados en asuntos tales como la divisibilidad, unicidad de la factorización y los números primos en lugar de asuntos referentes a la estructura de los grupos, anillos y campos que surgen en la teoría.

Los polinomios que se considerarán tendrán como coeficientes a números racionales. Tales polinomios se llaman polinomios sobre $R$, donde $R$ denota el campo de los números racionales. Frecuentemente se denota esta colección de polinomios por $R[x]$ y, más generalmente, el conjunto de todos los polinomios con coeficientes en un campo $F$ se denota por $F[x]$. Que el conjunto de números racionales forman un campo puede verificarse a partir de los postulados de la Sección 2.10. En un polinomio tal como

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n, \qquad a_0 \neq 0,$$

el entero no negativo $n$ recibe el nombre de grado del polinomio y $a_0$ es el coeficiente inicial. Si $a_0 = 1$, el polinomio se llama "mónico".

Dado que no se asigna grado al polinomio cero, puede asegurarse sin excepción que el grado del producto de dos polinomios es la suma de los grados de los polinomios.

Se dice que un polinomio $f(x)$ es divisible entre un polinomio $g(x)$, no idénticamente nulo, si existe un polinomio $q(x)$ tal que $f(x) = g(x)q(x)$ y se escribe

$$g(x)|f(x).$$

También se dice que $g(x)$ es un divisor o bien un factor de $f(x)$. El grado de $g(x)$ aquí no excede al de $f(x)$, a menos que $f(x)$ sea idénticamente cero, escrito $f(x) \equiv 0$. Este concepto de divisibilidad no es el mismo que el de la divisibilidad considerado anteriormente. En efecto, $3|7$ se cumple si 3 y 7 se consideran como polinomios de grado cero, mientras que no es cierto que el entero 3 divide al entero 7.

**Teorema 9.1** *A polinomios cualesquiera $f(x)$ y $g(x)$ sobre $R$ con $g(x) \not\equiv 0$ les corresponde los polinomios únicos $q(x)$ y $r(x)$ tales que $f(x) = g(x)q(x) + r(x)$, donde $r(x) \equiv 0$ o bien $r(x)$ es de grado menor que $g(x)$.*

*Demostración.* En el caso $f(x) \equiv 0$ o bien $f(x)$ tiene grado menor que $g(x)$, definimos $q(x) \equiv 0$ y $r(x) = f(x)$. De otra manera se divide $g(x)$ entre $f(x)$ para obtener un cociente $q(x)$ y un residuo $r(x)$. Evidentemente $q(x)$ y $r(x)$ son polinomios sobre $R$ y ya sea $r(x) \equiv 0$ o bien el grado de $r(x)$ es menor que el grado de $g(x)$ si se ha llevado a cabo la división hasta terminar. Si hubiera otro par, $q_1(x)$ y $r_1(x)$, entonces se tendría

$$f(x) = g(x)q_1(x) + r_1(x), \qquad r(x) - r_1(x) = g(x)\{q_1(x) - q(x)\}.$$

Así que $g(x)$ sería un divisor del polinomio $r(x) - r_1(x)$ el cual, a menos que sea idénticamente cero, tiene grado menor que $g(x)$. De aquí que $r(x) - r_1(x) \equiv 0$ y que concluye que $g(x) = q_1(x)$.

**Teorema 9.2** *Polinomios cualesquiera $f(x)$ y $g(x)$, no ambos idénticamente cero, tienen un divisor común $h(x)$ el cual es una combinación lineal de $f(x)$ y $g(x)$. De donde $h(x)|f(x)$, $h(x)|g(x)$, y*

$$h(x) = f(x)F(x) + g(x)G(x) \tag{9.1}$$

*para algunos polinomios $F(x)$ y $G(x)$.*

*Demostración.* De todos los polinomios de la forma (9.1) que no sean idénticamente cero, escoger cualquiera de grado menor y designarlo por $h(x)$. Si $h(x)$ no fuera divisor de $f(x)$, el Teorema 9.1 daría $f(x) = h(x)q(x) + r(x)$ con $r(x) \not\equiv 0$ y $r(x)$ de grado menor que $h(x)$. Pero entonces $r(x) = f(x) - h(x)q(x) = f(x)\{1 - F(x)q(x)\} - g(x)$

$\{G(x)q(x)\}$ el cual es de la forma (9.1) en contradicción con la selección de $h(x)$. Por tanto, $h(x)|f(x)$ y de modo semejante $h(x)|g(x)$.

**Teorema 9.3** *A polinomios cualesquiera* $f(x)$ *y* $g(x)$, *no ambos cero, les corresponde un polinomio mónico* $d(x)$ *que tiene las propiedades*

1) $d(x)|f(x)$, $d(x)|g(x)$;
2) $d(x)$ *es una combinación lineal de* $f(x)$ *y* $g(x)$, *como en* (9.1);
3) *todo divisor común de* $f(x)$ *y* $g(x)$ *es un divisor de* $d(x)$ *y, por tanto, no existe divisor común que tenga grado mayor al de* $d(x)$.

*Demostración.* Definir $d(x) = c^{-1}h(x)$, donde $c$ es el coeficiente inicial de $h(x)$, de modo que $d(x)$ es mónico. Las propiedades (1) y (2) se heredan de $h(x)$ y de $d(x)$. La ecuación (9.1) implica que $d(x) = c^{-1}f(x)F(x) + c^{-1}g(x)G(x)$ y esta ecuación muestra que si $m(x)$ es un divisor común de $f(x)$ y $g(x)$, entonces $m(x)|d(x)$. Finalmente, para probar que $d(x)$ es único, supóngase que tanto $d(x)$ como $d_1(x)$ satisfacen las propiedades (1), (2), (3). Entonces se tiene $d(x)|d_1(x)$ y $d_1(x)|d(x)$, de donde $d_1(x) = q(x)d(x)$ *y* $d(x) = q_1(x)d_1(x)$ para algunos polinomios $q(x)$ y $q_1(x)$. Esto implica que $q(x)q_1(x) = 1$, de lo cual se ve que $q(x)$ *y* $q_1(x)$ son de grado cero. Dado que tanto $d(x)$ como $d_1(x)$ son mónicos, se tiene $q(x) = 1$, $d_1(x) = d(x)$.

**Definición 9.1** *El polinomio* $d(x)$ *recibe el nombre de máximo común divisor de* $f(x)$ y $g(x)$. *Se escribe* $(f(x), g(x)) = d(x)$.

**Definición 9.2** *Un polinomio* $f(x)$, *no idénticamente cero, es irreducible, o bien primo, sobre* $R$ *si no existe factorización,* $f(x) = g(x)h(x)$, de $f(x)$ *en dos polinomios* $g(x)$ *y* $h(x)$ *de grados positivos sobre* $R$.

Por ejemplo, $x^2 - 2$ es irreducible sobre $R$. Tiene la factorización $(x - \sqrt{2})$ $(x + \sqrt{2})$ sobre el campo de los números reales, pero no tiene factorización sobre $R$.

**Teorema 9.4** *Si un polinomio irreducible* $p(x)$ *divide a un producto* $f(x)g(x)$, *entonces* $p(x)$ *divide por lo menos a uno de los polinomios* $f(x)$ *y* $g(x)$.

*Demostración.* Si $f(x) \equiv 0$ o bien $g(x) \equiv 0$ el resultado es obvio. Si ninguno es idénticamente cero, supongamos que $p(x) \nmid f(x)$ y probemos que $p(x)|g(x)$. La suposición de que $p(x) \nmid f(x)$ implica que $(p(x), f(x)) = 1$ y de aquí que por el Teorema 9.3 existen los polinomios $F(x)$ y $G(x)$ tales que $1 = p(x)F(x) + f(x)G(x)$. Multiplicando por $g(x)$ se obtiene

$$g(x) = p(x)g(x)F(x) + f(x)g(x)G(x).$$

Ahora bien, $p(x)$ es un divisor del segundo miembro de esta ecuación debido a que $p(x)|f(x)g(x)$ y de donde $p(x)|g(x)$.

**Teorema 9.5** *Todo polinomio $f(x)$ sobre $R$ de grado positivo puede factorizarse en un producto $f(x) = cp_1(x)p_2(x) \cdots p_k(x)$ donde los $p_j(x)$ son polinomios mónicos irreducibles sobre $R$. Esta factorización es única independientemente del orden.*

*Demostración.* Evidentemente $f(x)$ puede factorizarse repetidamente hasta convertirlo en un producto de polinomios irreducibles y la constante $c$ puede ajustarse de manera que todos los factores sean mónicos. Debemos probar la unicidad. Considérese otra factorización, $f(x) = cq_1(x)q_2(x) \cdots q_j(x)$, en polinomios mónicos irreducibles. De acuerdo con el Teorema 9.4, $p_1(x)$ divide a algún $q_i(x)$ y pueden reordenarse los $q_m(x)$ para hacer que $p_1(x)|q_1(x)$. Supuesto que $p_1(x)$ y $q_1(x)$ son irreducibles y mónicos, se tiene $p_1(x) = q_1(x)$. Una repetición de este argumento proporciona

$$p_2(x) = q_2(x), \quad p_3(x) = q_3(x), \quad \cdots \quad \text{y} \quad k = j$$

**Definición 9.3** *Se dice que un polinomio $f(x) = a_0x^n + \cdots + a_n$ con coeficientes enteros $a_j$ es primitivo si el máximo común divisor de sus coeficientes es* 1. *Obviamente, aquí debe entenderse el máximo común divisor de los enteros como se definió en la definición* 1.2.

**Teorema 9.6** *El producto de los polinomios primitivos es primitivo.*

*Demostración.* Sean $a_0x^n + \cdots + a_n$ y $b_0x^m + \cdots + b_m$ polinomios primitivos y denotemos su producto por $c_0x^{n+m} + \cdots + c_{n+m}$. Supóngase que este producto polinomial no es primitivo, de modo que existe un primo $p$ el cual divide todo coeficiente $c_k$. Supuesto que $a_0x^n + \cdots + a_n$ es primitivo, por lo menos uno de sus coeficientes no es divisible entre $p$. Denotemos por $a_i$ el primero de tales coeficientes y por $b_j$ el primer coeficiente de $b_0x^m + \cdots + b_m$ no divisible por $p$. Entonces el coeficiente de $x^{n+m-i-j}$ en el producto polinomial es

$$c_{i+j} = \sum a_k b_{i+j-k} \tag{9.2}$$

sumando sobre todo $k$ tal que $0 \leqq k \leqq n$, $0 \leqq i + j - k \leqq m$. En esta suma, todo término con $k < i$ es un múltiplo de $p$. Todo término con $k > i$ que aparece en la suma tendrá el factor $b_{i+j-k}$ con $i + j - k < j$ y también será un múltiplo de $p$. El término $a_ib_j$, para $k = i$, aparece en la suma y se tiene $c_{i+j} \equiv a_ib_j \pmod{p}$. Pero esto es una contradicción con $p|c_{i+j}$, $p \nmid a_i$, $p \nmid b_j$.

**Teorema 9.7** *Lema de Gauss. Si un polinomio mónico $f(x)$ con coeficientes enteros se factoriza en dos polinomios mónicos con coeficientes racionales, digamos $f(x) = g(x)h(x)$, entonces $g(x)$ y $h(x)$ tienen coeficientes enteros.*

*Demostración.* Si $g(x) = x^n + a_1x^{n-1} + \cdots + a_n$, los $a_i$ son racionales. Sea $k$ cualquier múltiplo común positivo de todos los denominadores de los $a_i$. Entonces $kg(x)$ tiene coeficientes enteros. Si $d$ es el máximo común divisor de los coeficientes de $kg(x)$, entonces $d$ divide al coeficiente inicial $k$ de $kg(x)$. Tomando $c = k/d > 0$, se ve que $cg(x)$ es un polinomio primitivo. De modo semejante existe un entero $c_1 > 0$ tal que $c_1h(x)$ es un polinomio primitivo. Entonces, por el Teorema 9.6, el producto $\{cg(x)\}\{c_1h(x)\} = cc_1f(x)$ es primitivo. Pero, supuesto que $f(x)$ tiene coeficientes enteros, esto implica que $cc_1 = 1$, de aquí que $c = c_1 = 1$.

**Problemas**

1. Si $f(x)|g(x)$ y $g(x)|f(x)$, probar que existe un número racional $c$ tal que $g(x) = cf(x)$.
2. Si $f(x)|g(x)$ y $g(x)|h(x)$, probar que $f(x)|h(x)$.
3. Si $p(x)$ es irreducible y $g(x)|p(x)$, probar que $g(x)$ es una constante o bien $g(x) = cp(x)$ para algún número racional $c$.
4. Si $p(x)$ es irreducible, probar que $cp(x)$ es irreducible para todo racional $c \neq 0$.
5. Si un polinomio $f(x)$ con coeficientes enteros se factoriza en un producto $g(x)h(x)$ de dos polinomios con coeficientes en $R$, probar que existe una factorización $g_1(x)h_1(x)$ con coeficientes enteros.
6. Si $f(x)$ y $g(x)$ son polinomios primitivos y si $f(x)|g(x)$ y $g(x)|f(x)$, probar que $f(x) = \pm g(x)$.

## 9.2 Números algebraicos

**Definición 9.4** *Un número complejo $\xi$ recibe el nombre de número algebraico si satisface alguna ecuación polinomial $f(x) = 0$ donde $f(x)$ es un polinomio sobre $R$.*

Todo número racional $r$ es un número algebraico debido a que en este caso $f(x)$ puede tomarse como $x - r$.

**Teorema 9.8** *Un número algebraico $\xi$ satisface una ecuación polinomial mónica irreducible única $g(x) = 0$ sobre $R$. Además toda ecuación polinomial sobre $R$ satisfecha por $\xi$ es divisible entre $g(x)$.*

*Demostración.* De todas las ecuaciones polinomiales sobre $R$ satisfechas por $\xi$, escojamos una de menor grado digamos $G(x) = 0$. Si el coeficiente inicial de $G(x)$ es $c$, definimos $g(x) = c^{-1}G(x)$, de modo

que $g(\xi) = 0$ y $g(x)$ es mónico. El polinomio $g(x)$ es irreducible, porque si $g(x) = h_1(x)h_2(x)$, entonces se cumpliría por lo menos uno de $h_1(\xi) = 0$ y $h_2(\xi) = 0$, contrario al hecho de que $G(x) = 0$ y $g(x) = 0$ son ecuaciones polinomiales sobre $R$ de grado menor satisfechas por $\xi$.

A continuación sea $f(x) = 0$ cualquier ecuación polinomial sobre $R$ que tiene a $\xi$ como una raíz. Aplicando el Teorema 9.1 se obtiene $f(x) = g(x)q(x) + r(x)$. El residuo $r(x)$ debe ser idénticamente cero, porque de otro modo el grado de $r(x)$ sería menor que el de $g(x)$ y $\xi$ sería una raíz de $r(x)$ supuesto que $f(\xi) = g(\xi) = 0$. De aquí que $g(x)$ es un divisor de $f(x)$.

Finalmente, para probar que $g(x)$ es único supóngase que $g_1(x)$ es un polinomio mónico irreducible tal que $g_1(\xi) = 0$. Entonces, por el argumento anterior, $g(x)|g_1(x)$ digamos $g_1(x) = g(x)q(x)$. Pero la irreducibilidad de $g_1(x)$ entonces implica que $q(x)$ es una constante, de hecho $q(x) = 1$ dado que $g_1(x)$ y $g(x)$ son mónicos. Así se tiene $g_1(x) = g(x)$.

**Definición 9.5** *La ecuación mínima de un número algebraico $\xi$ es la ecuación $g(x) = 0$ descrita en el Teorema* 9.8. *El polinomio mínimo de $\xi$ es $g(x)$. El grado de un número algebraico es el grado de su polinomio mínimo.*

**Definición 9.6** *Un número algebraico $\xi$ es un entero algebraico si satisface alguna ecuación polinomial mónica*

$$f(x) = x^n + b_1x^{n-1} + \cdots + b_n = 0 \tag{9.3}$$

*con coeficientes enteros.*

**Teorema 9.9** *Entre los números racionales, los únicos que son enteros algebraicos son los enteros* $0, \pm1, \pm2, \cdots$.

*Demostración.* Todo entero $m$ es un entero algebraico debido a que $f(x)$ puede tomarse como $x - m$. Por otra parte, si cualquier número racional $m/q$ es un entero algebraico, entonces puede suponerse $(m, q) = 1$ y se tiene

$$\left(\frac{m}{q}\right)^n + b_1\left(\frac{m}{q}\right)^{n-1} + \cdots + b_n = 0,$$

$$m^n + b_1qm^{n-1} + \cdots + b_nq^n = 0.$$

Así que $q|m^n$, de manera que $q = \pm1$ y $m/q$ es un entero.

Así la palabra "entero" de la definición 9.6 es simplemente una generalización de nuestro uso previo. En la teoría de los números algebraicos, $0, \pm1, \pm2, \cdots$ con frecuencia se le da el nombre de "enteros racionales" para distinguirlos de los otros enteros algebraicos, que no son

racionales. Por ejemplo, $\sqrt{2}$ es un entero algebraico pero no un entero racional.

**Teorema 9.10** *La ecuación mínima de un entero algebraico es mónica con coeficientes enteros.*

*Demostración.* La ecuación es mónica por definición, de manera que sólo es necesario probar que los coeficientes son enteros. Supongamos que el entero algebraico $\xi$ satisface $f(x) = 0$ como en (9.3) y sea su ecuación mínima $g(x) = 0$, mónica e irreducible sobre $R$. Por el Teorema 9.8, $g(x)$ es un divisor de $f(x)$, digamos $f(x) = g(x)h(x)$, y el cociente $h(x)$, como $f(x)$ y $g(x)$, son mónicos y tienen coeficientes en $R$. Aplicando el Teorema 9.7, se ve que $g(x)$ tiene coeficientes enteros.

**Teorema 9.11** *Sea $n$ un entero racional positivo y $\xi$ un número complejo. Supóngase que los números complejos $\theta_1, \theta_2, \cdots, \theta_n$, no todos cero, satisfacen las ecuaciones*

$$(9.4) \quad \xi\theta_j = a_{j,1}\theta_1 + a_{j,2}\theta_2 + \cdots + a_{j,n}\theta_n, \qquad j = 1, 2, \cdots, n,$$

*donde los $n^2$ coeficientes $a_{j,i}$ son racionales. Entonces $\xi$ es un número algebraico. Es más, si los $a_{j,i}$ son enteros racionales, $\xi$ es un entero algebraico.*

*Demostración.* Las ecuaciones (9.4) pueden pensarse como un sistema de ecuaciones lineales homogéneas en $\theta_1, \theta_2, \cdots, \theta_n$. Supuesto que no todos los $\theta_i$ son cero, el determinante de los coeficientes debe nulificarse:

$$\begin{vmatrix} \xi - a_{1,1} & -a_{1,2} & \cdots & a_{1,n} \\ -a_{2,1} & \xi - a_{2,2} & \cdots & -a_{2,n} \\ \cdots & \cdots & \cdots & \cdots \\ -a_{n,1} & -a_{n,2} & \cdots & \xi - a_{n,n} \end{vmatrix} = 0.$$

El desarrollo de esta determinante da una ecuación $\xi^n + b_1\xi^{n-1} + \cdots + b_n = 0$, donde los $b_i$ son polinomios en los $a_{j,k}$. De donde los $b_i$ son racionales y son enteros racionales si los $a_{j,k}$ lo son.

**Teorema 9.12** *Si $\alpha$ y $\beta$ son números algebraicos, lo son $\alpha + \beta$ y $\alpha\beta$. Si $\alpha$ y $\beta$ son enteros algebraicos, lo son $\alpha + \beta$ y $\alpha\beta$.*

*Demostración.* Supóngase que $\alpha$ y $\beta$ satisfacen

$$\alpha^m + a_1\alpha^{m-1} + \cdots + a_m = 0,$$
$$\beta^r + b_1\beta^{r-1} + \cdots + b_r = 0$$

con coeficientes racionales $a_i$ y $b_j$. Sea $n = mr$ y definamos los números complejos $\theta_1, \cdots, \theta_n$ como los números

$$\begin{array}{ccccc} 1, & \alpha, & \alpha^2, & \cdots, & \alpha^{m-1}, \\ \beta, & \alpha\beta, & \alpha^2\beta, & \cdots, & \alpha^{m-1}\beta, \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ \beta^{r-1}, & \alpha\beta^{r-1}, & \alpha^2\beta^{r-1}, & \cdots, & \alpha^{m-1}\beta^{r-1}, \end{array}$$

en cualquier orden. Así $\theta_1, \cdots, \theta_n$ son los números $\alpha^s\beta^t$ con $s = 0, 1, \cdots, m-1$ y $t = 0, 1, \cdots, r-1$. De aquí que para todo $\theta_j$,

$$\alpha\theta_j = \alpha^{s+1}\beta^t = \begin{cases} \text{algún } \theta_k & \text{si} \quad s+1 \leqq m-1 \\ (-a_1\alpha^{m-1} - a_2\alpha^{m-2} - \cdots - a_m)\beta^t & \text{si} \quad s+1 = m. \end{cases}$$

En ambos casos se ve que existen las constantes racionales $h_{j,1}, \cdots, h_{j,n}$ tales que $\alpha\theta_j = h_{j,1}\theta_1 + \cdots + h_{j,n}\theta_n$. De modo semejante, existen las constantes racionales $k_{j,1} \cdots, k_{j,n}$ tales que $\beta\theta_j = k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n$ y de aquí que $(\alpha + \beta)\theta_j = (h_{j,1} + k_{j,1})\theta_1 + \cdots + (h_{j,n} + k_{j,n})\theta_n$. Estas ecuaciones son de la forma (9.4) y así se concluye que $\alpha + \beta$ es algebraico. Además, si $\alpha$ y $\beta$ son enteros algebraicos, entonces los $a_j$, $b_j$, $h_{j,i}$, $k_{j,i}$ son todos enteros racionales y $\alpha + \beta$ es un entero algebraico.

También se tiene $\alpha\beta\theta_j = \alpha(k_{j,1}\theta_1 + \cdots + k_{j,n}\theta_n) = k_{j,1}\alpha\theta_1 + \cdots + k_{j,n}\alpha\theta_n$ de lo cual se encuentra $\alpha\beta\theta_j = c_{j,1}\theta_1 + \cdots + c_{j,n}\theta_n$ donde $c_{j,i} = k_{j,1}h_{1,i} + k_{j,2}h_{2,i} + \cdots + k_{j,n}h_{n,i}$. Una vez más se aplica el teorema 9.11 para concluir que $\alpha\beta$ es algebraico y que es un entero algebraico si $\alpha$ y $\beta$ lo son.

Este teorema establece que el conjunto de números algebraicos es cerrado bajo la adición y la multiplicación y, del mismo modo, para el conjunto de los enteros algebraicos. El siguiente resultado establece un poco más

**Teorema 9.13** *El conjunto de todos los números algebraicos forma un campo. La clase de todos los enteros algebraicos forma un anillo.*

*Demostración.* Los anillos y los campos se definen en la definición 2.12. Los números racionales 0 y 1 sirven como el cero y la unidad para el sistema. Se ve fácilmente que la mayoría de los postulados se satisfacen si se recuerda que los números algebraicos son números complejos cuyas propiedades nos son familiares. El único lugar donde se presenta alguna dificultad es al probar la existencia de los inversos aditivos y multiplicativos. Si $\alpha \neq 0$ es una solución de

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

entonces $-\alpha$ y $\alpha^{-1}$ son soluciones de

$$a_0x^n - a_1x^{n-1} + a_2x^{n-2} - \cdots + (-1)^n a_n = 0$$

y

$$a_0 + a_1x + a_2x^2 + \cdots + a_nx^n = 0,$$

respectivamente. Por lo tanto, si $\alpha$ es un número algebraico, entonces lo son $-\alpha$ y $\alpha^{-1}$. Si $\alpha$ es un entero algebraico, entonces lo es $-\alpha$, pero no necesariamente $\alpha^{-1}$. Por lo tanto, los números algebraicos forman un campo, los enteros algebraicos un anillo.

**Problemas**

1. Encontrar el polinomio mínimo de cada uno de los siguientes números algebraicos: 7, $\sqrt[3]{7}$, $(1 + \sqrt[3]{7})/2$, $1 + \sqrt{2} + \sqrt{3}$. ¿Cuáles de éstos son enteros algebraicos?
2. Probar que si $\alpha$ es algebraico de grado $n$, entonces $-\alpha, \alpha^{-1}$ y $\alpha - 1$ también son de grado $n$.
3. Probar que si $\alpha$ es algebraico de grado $n$ y $\beta$ es algebraico de grado $m$, entonces $\alpha + \beta$ es de grado $\leqq mn$. Probar un resultado semejante para $\alpha\beta$.
4. Probar que el conjunto de todos los números algebraicos reales (a saber, los números algebraicos que son reales) forman un campo y el conjunto de todos los enteros algebraicos reales forma un anillo.

## 9.3 Campos de números algebraicos

El campo discutido en el teorema 9.13 contiene la totalidad de los números algebraicos. En general un campo de números algebraicos es todo subconjunto de esta colección total que es él mismo un campo. Por ejemplo, si $\xi$ es un número algebraico, entonces puede verificarse rápidamente que la colección de todos los números de la forma $f(\xi)/h(\xi)$, $h(\xi) \neq 0$, $f$ y $h$ polinomios sobre $R$, constituye un campo. Este campo se denota por $R(\xi)$ y se llama la extensión de $R$ por $\xi$.

**Teorema 9.14** *Si $\xi$ es un número algebraico de grado $n$, entonces todo número en $R(\xi)$ puede escribirse unívocamente en la forma*

$$(9.5) \qquad a_0 + a_1\xi + \cdots + a_{n-1}\xi^{n-1}$$

*donde los $a_i$ son números racionales.*

*Demostración.* Considérese cualquier número $f(\xi)/h(\xi)$ de $R(\xi)$. Si el polinomio mínimo de $\xi$ es $g(x)$, entonces $g(x) \nmid h(x)$, por el teorema 9.8, dado que $h(\xi) \neq 0$. Pero $g(x)$ es irreducible, de modo que el polinomio máximo común divisor de $g(x)$ y $h(x)$ es 1 y por tanto, por el teorema 9.3, existen los polinomios $G(x)$ y $H(x)$ tales que $1 = g(x)G(x) + h(x)H(x)$. Reemplazando $x$ por $\xi$ y aplicando el hecho de que $g(\xi) = 0$ se obtiene $1/h(\xi) = H(\xi)$ y $f(\xi)/h(\xi) = f(\xi)H(\xi)$. Sea $k(x) = f(x)H(x)$ de manera que $f(\xi)/h(\xi) = k(\xi)$. Dividiendo $k(x)$ por $g(x)$ se obtiene $k(x) = g(x)q(x) + r(x)$ y de aquí que $f(\xi)/h(\xi) = k(\xi) = r(\xi)$ donde $r(\xi)$ es de la forma (9.5).

Para probar que la forma (9.5) es única, supóngase que $r(\xi)$ y $r_1(\xi)$ son expresiones de la forma (9.5). Si $r(x) - r_1(x)$ no es idénticamente cero, entonces es un polinomio de grado menor que $n$. Dado que el polinomio mínimo de $\xi$ tiene grado $n$, se tiene $r(\xi) - r_1(\xi) \neq 0$, $r(\xi) \neq r_1(\xi)$, a menos que $r(x)$ y $r_1(x)$ sean el mismo polinomio.

El campo $R(\xi)$ puede mirarse en forma diferente, por consideración de las congruencias módulo el polinomio $g(x)$. Esto es, en analogía con la definición 2.1, para todo polinomio $G(x)$ de grado por lo menos uno, se escribirá

$$f_1(x) \equiv f_2(x) \pmod{G(x)}$$

si $G(x)|(f_1(x) - f_2(x))$. Finalmente, para regresar a $R(\xi)$ se tomará el polinomio mínimo $g(x)$ de $\xi$ para $G(x)$. Sin embargo, la teoría de las congruencias es más general y se parte del polinomio $G(x)$ sobre $R$, irreducible o no. Las propiedades de las congruencias dadas en el teorema 2.1 pueden extenderse inmediatamente al caso polinomial. Por ejemplo, la parte $(c)$ del teorema tiene la anóloga: si $f_1(x) \equiv f_2(x) \pmod{G(x)}$ y $h_1(x) \equiv h_2(x) \pmod{G(x)}$, entonces $f_1(x)h_1(x) \equiv f_2(x)h_2(x) \pmod{G(x)}$.

Por el algoritmo de la división, teorema 9.1, todo polinomio $f(x)$ sobre $R$ se mapea por la división entre $G(x)$ sobre un polinomio único $r(x)$ módulo $G(x)$;

$$f(x) = G(x)q(x) + r(x), \qquad f(x) \equiv r(x) \pmod{G(x)}.$$

Por tanto, el conjunto de polinomios $r(x)$ que consiste de 0 y todos los polinomios sobre $R$ de grado menor que $n$ constituye "un sistema completo de residuos módulo $G(x)$" en el sentido de la definición 2.2. Por supuesto que el sistema de residuos presente tiene un número infinito de miembros, mientras que el sistema de residuos módulo $m$ contiene precisamente $m$ elementos.

**Teorema 9.15** *Sea $G(x)$ un polinomio sobre $R$ de grado $n \geqq 1$. La totalidad de los polinomios*

$$r(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} \tag{9.6}$$

*con coeficientes en $R$ y con adición y multiplicación módulo $G(x)$ forma un anillo.*

*Demostración.* Este teorema es el análogo de la primera parte del teorema 2.33 y su demostración es virtualmente la misma. Primero se observa que los polinomios (9.6) forman un grupo bajo la adición, con elemento identidad 0, siendo $-r(x)$ el inverso aditivo de $r(x)$. A continuación, los polinomios (9.6) son cerrados bajo la multiplicación módulo $G(x)$ y la propiedad asociativa de la multiplicación se obtiene de la

propiedad correspondiente para los polinomios sobre $R$ con la multiplicación ordinaria, esto es

$$\{r_1(x)r_2(x)\}r_3(x) = r_1(x)\{r_2(x)r_3(x)\}$$

implica

$$\{r_1(x)r_2(x)\}r_3(x) \equiv r_1(x)\{r_2(x)r_3(x)\} \pmod{G(x)}.$$

De modo semejante, la propiedad distributiva módulo $G(x)$ se hereda de la propiedad distributiva de los polinomios sobre $R$.

Antes de establecer el siguiente teorema, extenderemos la definición 2.10 al concepto de isomorfismo entre campos. Dos campos $F$ y $F'$ son isomorfos si existe una correspondencia biunívoca entre los elementos de $F$ y los elementos de $F'$ tal que si $a$ y $b$ en $F$ corresponden respectivamente a $a'$ y $b'$ en $F'$, entonces $a + b$ y $ab$ en $F$ corresponden respectivamente a $a' + b'$ y $a'b'$ en $F'$. Se aplica una definición virtualmente idéntica para el concepto de isomorfismo entre anillos. El resultado siguiente es un análogo directo de la segunda parte del teorema 2.33.

**Teorema 9.16** *El anillo de polinomios módulo $G(x)$ descrito en el teorema* 9.15 *es un campo si, y solamente si, $G(x)$ es un polinomio irreducible. Si $G(x)$ es el polinomio mínimo del número algebraico $\xi$, entonces este campo es isomorfo a $R(\xi)$.*

*Demostración.* Si el polinomio $G(x)$ es reducible sobre $R$, digamos $G(x) = G_1(x)G_2(x)$ donde $G_1(x)$ y $G_2(x)$ tienen grados entre 1 y $n - 1$, entonces $G_1(x)$ y $G_2(x)$ son de la forma (9.6). Pero entonces $G_1(x)$ no tiene inverso multiplicativo módulo $G(x)$ dado que $G_1(x)f(x) \equiv 1 \pmod{G(x)}$ implica

$$G(x)|\{G_1(x)f(x) - 1\}, \quad G_1(x)|\{G_1(x)f(x) - 1\}, \quad G_1(x)|1.$$

De aquí que el anillo de polinomios módulo $G(x)$ no es un campo.

Por otra parte, si $G(x)$ es irreducible sobre $R$, entonces todo polinomio $r(x)$ de la forma (9.6) tiene un inverso multiplicativo único $r_1(x)$ módulo $G(x)$, de la forma (9.6). Para demostrar esto se observa que el máximo común divisor de $G(x)$ y $r(x)$ es 1 y así, por el teorema 9.3, existen los polinomios $f(x)$ y $h(x)$ tales que

$$1 = r(x)f(x) + G(x)h(x). \tag{9.7}$$

Aplicando el teorema 9.1 a $f(x)$ y $G(x)$ se obtiene $f(x) = G(x)q(x) + r_1(x)$ donde $r_1(x)$ es de la forma (9.6). Así que (9.7) puede escribirse

$$1 = r(x)r_1(x) + G(x)\ \{h(x) + r(x)q(x)\}, \quad r(x)r_1(x) \equiv 1 \pmod{G(x)},$$

de modo que $r_1(x)$ es un inverso multiplicativo de $r(x)$ de la forma (9.6). Este inverso es único porque si $r(x)r_2(x) \equiv 1 \pmod{G(x)}$ entonces

$$r(x)r_1(x) \equiv r(x)r_2(x) \pmod{G(x)}, \qquad G(x)|r(x)\ \{r_1(x) - r_2(x)\}.$$

Supuesto que $G(x) \not| r(x)$, por el teorema 9.4, se tiene $G(x)\{r_1(x) - r_2(x)\}$. Pero el polinomio $r_1(x) - r_2(x)$ es idénticamente cero o bien es de grado menor que $n$, el grado de $G(x)$. De donde $r_1(x) - r_2(x) = 0$, $r_1(x) = r_2(x)$.

Finalmente, si $G(x)$ es el polinomio mínimo $g(x)$ del número algebraico $\xi$, debe demostrarse que el campo es isomorfo a $R(\xi)$. A cada $r(x)$ de la forma (9.6) le hacemos corresponder el número $r(\xi)$ de $R(\xi)$. El Teorema 9.15 muestra que esta correspondencia es biunívoca. Si

$$r_1(x)r_2(x) \equiv r_3(x), \quad r_1(x) + r_2(x) \equiv r_4(x) \pmod{G(x)},$$

entonces

$$r_1(x)r_2(x) = r_3(x) + q_1(x)G(x), r_1(x) + r_2(x) = r_4(x) + q_2(x)G(x),$$

y de aquí que

$$r_1(\xi)r_2(\xi) = r_3(\xi), \quad r_1(\xi) + r_3(\xi) = r_4(\xi),$$

supuesto que $G(\xi) = 0$. Por lo tanto, la correspondencia conserva la multiplicación y la adición.

El teorema que se acaba de probar es significativo en que hace posible el desarrollo de la teoría de los números algebraicos a partir de la consideración de los polinomios sin referencia alguna a las raíces de los polinomios. El teorema fundamental del álgebra establece que todo polinomio de grado positivo sobre $R$ tiene una raíz que es un número complejo. Por tanto, los campos de números algebraicos obtenidos por medio del Teorema 9.16 son esencialmente los mismos que —isomorfos a— los campos $R(\xi)$ del Teorema 9.14, pero no es necesario conocer el teorema fundamental del álgebra para aplicar el método del Teorema 9.16.

El teorema fundamental del álgebra implica, y en ocasiones se establece en la forma, que todo polinomio $f(x)$ de grado $n$ sobre $R$ tiene $n$ raíces complejas. Si $f(x)$ es irreducible sobre $R$, entonces las $n$ raíces, digamos $\xi_1 \cdots, \xi_n$, se llaman números algebraicos conjugados y los conjugados de cualquiera de ellos son simplemente todos los demás. Ahora bien, el Teorema 9.16 no hace distinción alguna entre los conjugados, mientras que el Teorema 9.14 tiene en cuenta esa distinción. Por ejemplo, sea $g(x)$ el polinomio irreducible $x^3 - 2$. En el Teorema 9.14 puede tomarse $\xi$ como cualquiera de los tres números algebraicos que son soluciones de $x^3 - 2 = 0$, a saber $\sqrt[3]{2}$, $\omega\ \sqrt[3]{2}$, $\omega^2\ \sqrt[3]{2}$ donde $\omega = (-1 + i\sqrt{3})/2$. Por tanto, existen tres campos

(9.8) $$R(\sqrt[3]{2}), \quad R(\omega\sqrt[3]{2}), \quad R(\omega^2\sqrt[3]{2}).$$

El primero de éstos consiste de los números reales, mientras que los otros dos contienen elementos no reales. Por lo tanto, el primero es evidentemente un campo diferente de los otros. No es tan evidente, pero puede probarse, que los dos últimos difieren uno respecto al otro. Por otra parte, si se aplica el Teorema 9.16 al polinomio $x^3 - 2$ se obtiene un solo campo que consiste de todos los polinomios $a_0 + a_1x + a_2x^2$ sobre $R$ módulo $x^3 - 2$. De acuerdo con el Teorema 9.16, este campo es isomorfo a cada uno de los campos (9.8). Dado que el isomorfismo es una propiedad transitiva, los campos (9.8) son isomorfos uno respecto al otro. Difieren en que contienen elementos diferentes, pero son esencialmente los mismos excepto por los nombres de sus elementos.

**Problemas**

1. Probar que los campos de (9.8), aunque isomorfos, son distintos. *Sugerencia:* para probar que $R(\omega^2 \sqrt[3]{2})$ es diferente de $R(\omega \sqrt[3]{2})$, supóngase que $\omega^2 \sqrt[3]{2}$ es un elemento del último campo, esto es, supóngase que existen los racionales $a$, $b$, $c$ tales que $\omega^2 \sqrt[3]{2} = a + b\omega \sqrt[3]{2} + c(\omega\sqrt[3]{2})^2$. Probar que no existen tales racionales.
2. Probar que el campo $R(i)$, donde $i^2 = -1$, es isomorfo al campo de todos los polinomios $a + bx$ con $a$ y $b$ en $R$, tomado el módulo $x^2 + 1$.
3. Probar que todo campo de números algebraicos contiene a $R$ como un subcampo.
4. Suponiendo el teorema fundamental del álgebra, probar el Teorema 9.10 mediante el procedimiento siguiente. Supóngase que el entero algebraico $\xi$ satisface alguna ecuación polinomial mónica $f(x) = 0$ con coeficientes enteros. Entonces puede factorizarse $f(x)$ en el campo de los números complejos, digamos
$$f(x) = (x - \xi)(x - \xi_2)(x - \xi_3) \cdots (x - \xi_n).$$
Si $g(x)$ es el polinomio mínimo de $\xi$, entonces $g(x)|f(x)$ por el Teorema 9.8, y así
$$g(x) = (x - \xi)(x - \theta_2) \cdots (x - \theta_r)$$
donde $\theta_2, \cdots, \theta_r$ son un subconjunto de $\xi_2, \cdots, \xi_n$. Así que $\xi, \theta_2, \cdots, \theta_r$ son enteros algebraicos y por el Teorema 9.12, los coeficientes de $g(x)$ son enteros algebraicos. A continuación aplíquese el Teorema 9.9.

## 9.4 Enteros algebraicos

Todo campo de números algebraicos contiene los elementos 0, y 1 y así, por los postulados para un campo, debe contener todos los números racionales. De donde todo campo de números algebraicos contiene por lo menos algunos enteros algebraicos, los enteros racionales 0, $\pm1$, $\pm2$, $\cdots$. El resultado siguiente muestra que, en general, un campo de números algebraicos también contiene otros enteros algebraicos.

**Teorema 9.17** *Si $\alpha$ es cualquier número algebraico, existe un entero racional $b$ tal que $b\alpha$ es un entero algebraico.*

*Demostración.* Sea $f(x)$ un polinomio sobre $R$ tal que $f(\alpha) = 0$. Puede suponerse que los coeficientes de $f(x)$ son enteros racionales, puesto que puede multiplicarse por el mínimo común múltiplo de los denominadores de los coeficientes. Así que puede tomarse $f(x)$ en la forma

$$f(x) = bx^n + a_1x^{n-1} + \cdots + a_n = bx^n + \sum_{j=1}^{n} a_jx^{n-j}$$

con enteros racionales $b$ y $a_j$. Entonces $b\alpha$ es un cero de

$$b^{n-1}f\left(\frac{x}{b}\right) = x^n + \sum_{j=1}^{n} a_jb^{j-1}x^{n-j},$$

y de aquí que $b\alpha$ es un entero algebraico.

**Teorema 9.18** *Los enteros de todo campo de números algebraicos forman un anillo.*

*Demostración.* Si $\alpha$ y $\beta$ son enteros en un campo $F$ así, entonces $\alpha + \beta$ y $\alpha\beta$ están en $F$ supuesto que $F$ es un campo. Pero, por los Teoremas 9.12 y 9.13, $\alpha + \beta$, $\alpha\beta$ y $-\alpha$ son enteros algebraicos. De donde los enteros de $F$ forman un anillo con 0 y 1 como los elementos de la adición y la multiplicación.

**Definición 9.7** *En todo campo de números algebraicos $F$, se dice que un entero $\alpha \neq 0$ es un divisor de un entero $\beta$ si existe un entero $\gamma$ tal que $\beta = \alpha\gamma$. En este caso se escribe $a|\beta$. Todo divisor del entero 1 se llama unidad de $F$. Los enteros diferentes de cero $\alpha$ y $\beta$ se llaman asociados si $\alpha/\beta$ es una unidad.*

Esta definición de asociados no parece que sea simétrica en $\alpha$ y $\beta$ pero se establecerá que la propiedad realmente es simétrica.

**Teorema 9.19** *El recíproco de una unidad es una unidad. Las unidades de un campo de números algebraicos forman un grupo multiplicativo.*

*Demostración.* Si $\varepsilon_1$ es una unidad, entonces existe un entero $\varepsilon_2$ tal que $\varepsilon_1\varepsilon_2 = 1$. De aquí que $\varepsilon_2$ también es una unidad y es el recíproco de $\varepsilon_1$. Si, de modo semejante, $\varepsilon_3$ es cualquier unidad con recíproco $\varepsilon_4$, entonces el producto $\varepsilon_1\varepsilon_3$ es una unidad porque $(\varepsilon_1\varepsilon_3)(\varepsilon_2\varepsilon_4) = 1$. De aquí que las unidades de un campo de números algebraicos forman un grupo multiplicativo donde el elemento identidad es 1 y el inverso de $\varepsilon$ es el recíproco de $\varepsilon$.

Si $\alpha$ y $\beta$ son asociados, entonces $\alpha/\beta$ es una unidad por definición y, por el teorema anterior, $\beta/\alpha$ también es una unidad. De donde la definición de asociados es simétrica: si $\alpha$ y $\beta$ son asociados, entonces lo son $\beta$ y $\alpha$.

**Problemas**

1. Probar que las unidades del campo de números racionales $R$ son $\pm 1$ y que los enteros $\alpha$ y $\beta$ son asociados en este campo si y solamente si $\alpha = \pm\beta$.
2. Para cualquier número algebraico $\alpha$, definir $m$ como el menor entero positivo racional tal que $m\alpha$ es un entero algebraico. Probar que si $b\alpha$ es un entero algebraico, donde $b$ es un entero racional, entonces $m|b$.
3. Sea $\alpha = \alpha_1 + \alpha_2 i$ un número algebraico, donde $\alpha_1$ y $\alpha_2$ son reales. ¿Se concluye que $\alpha_1$ y $\alpha_2$ son números algebraicos? Si $\alpha$ es un entero algebraico, ¿serían $\alpha_1$ y $\alpha_2$ necesariamente enteros algebraicos?

## 9.5 Campos cuadráticos

Un campo cuadrático es uno de la forma $R(\xi)$ donde $\xi$ es una raíz de un polinomio cuadrático irreducible sobre $R$. Por el Teorema 9.14, los elementos de tal campo son la totalidad de los números de la forma $a_0 + a_1\xi$, donde $a_0$ y $a_1$ son números racionales. Dado que $\xi$ es de la forma $(a + b\sqrt{m})/c$ donde $a, b, c, m$ son enteros, se ve que

$$R(\xi) = R\left(\frac{a + b\sqrt{m}}{c}\right) = R(a + b\sqrt{m}) = R(b\sqrt{m}) = R(\sqrt{m})$$

Aquí se ha supuesto que $c \neq 0$ y que $m$ es exento de cuadrados, $m \neq 1$. Por otra parte, si $m$ y $n$ son dos enteros racionales diferentes exentos de cuadrados, ninguno de los cuales es 1, entonces $R(\sqrt{m}) \neq R(\sqrt{n})$ dado que $\sqrt{m}$ no está en $R(\sqrt{n})$. Esto es, es imposible encontrar los números racionales $b$ y $a$ tales que $\sqrt{m} = a + b\sqrt{n}$.

**Teorema 9.20** *Todo campo cuadrático es de la forma $R(\sqrt{m})$ donde $m$ es un entero racional exento de cuadrados, positivo o bien negativo pero no igual a* 1. *Los números de la forma $a + b\sqrt{m}$ con enteros racionales $a$ y $b$ son enteros de $R(\sqrt{m})$. Estos son los únicos enteros de $R(\sqrt{m})$ si $m \equiv 2$ o bien* 3 (mod 4). *Si $m \equiv 1$* (mod 4) *los números $(a + b\sqrt{m})/2$, con $a$ y $b$ enteros racionales impares, también son enteros de $R(\sqrt{m})$ y no existen más enteros.*

*Demostración.* Ya se ha probado la primera parte del teorema. Todo lo que falta es identificar los enteros algebraicos. Todo número en $R(\sqrt{m})$ es de la forma $\alpha = (a + b\sqrt{m})/c$ donde $a, b, c$, son

enteros racionales con $c > 0$. No se pierde generalidad al suponer que $(a, b, c) = 1$ de modo que $\alpha$ está en su más simple expresión. Si $b = 0$, entonces $\alpha$ es racional y, por el Teorema 9.9, es un entero algebraico si y solamente si es un entero racional, esto es $c = 1$. Si $b \neq 0$, entonces $\alpha$ no es racional y su ecuación mínima es cuadratica,

$$\left(x - \frac{a + b\sqrt{m}}{c}\right)\left(x - \frac{a - b\sqrt{m}}{c}\right) = x^2 - \frac{2a}{c}x + \frac{a^2 - b^2m}{c^2} = 0.$$

De acuero con el Teorema 9.10, entonces $\alpha$ será un entero algebraico si y sólo si esta ecuación es mónica con coeficientes enteros. De donde $\alpha$ es un entero algebraico si y sólo si

(9.9) $$c|2a \quad \text{y} \quad c^2|(a^2 - b^2m),$$

y esto incluye el caso $b = 0$, supuesto que $(a, b, c) = 1$. Si $(a, c) > 1$ y $c|2a$, entonces $a$ y $c$ tienen algún factor primo común, digamos $p$, y $p \nmid b$ supuesto que $(a, b, c) = 1$. Entonces $p^2|a^2$ y $p^2|c^2$, y si $c^2|(a^2 - b^2m)$, se tendría $p^2|b^2m$, $p^2|m$, lo cual es imposible dado que $m$ es exento de cuadrados. Por tanto, (9.9) puede cumplirse sólo si $(a, c) = 1$. Si $c|2a$ y $c > 2$ entonces $(a, c) > 1$, de manera que (9.9) sólo puede cumplirse si $c = 1$ o bien $c = 2$. Es obvio que (9.9) se cumple para $c = 1$. Para $c = 2$ la condición (9.9) se transforma en $a^2 \equiv b^2m \pmod 4$ y también se tiene $a$ impar puesto que $(a, c) = 1$. Entonces (9.9) se transforma en $b^2m \equiv a^2 \equiv 1 \pmod 4$, lo cual requiere que $b$ sea impar y entonces se reduce a $m \equiv b^2m \equiv 1 \pmod 4$. Para resumir: (9.9) se satisface si y solamente si $c = 1$ o bien $c = 2$, $a$ impar, $b$ impar, $m \equiv 1 \pmod 4$, y esto completa la demostración.

**Definición 9.8** *La norma $N(\alpha)$ de un número $\alpha = (a + b\sqrt{m})/c$ en $R(\sqrt{m})$ es el producto de $\alpha$ y su conjugado, $\bar{\alpha} = (a - b\sqrt{m})/c$,*

$$N(\alpha) = \alpha\bar{\alpha} = \frac{a + b\sqrt{m}}{c}\frac{a - b\sqrt{m}}{c} = \frac{a^2 - b^2m}{c^2}.$$

*Nótese que si $\alpha$ es un número racional en $R(\sqrt{m})$, entonces $\bar{\alpha} = \alpha$.*

**Teorema 9.21** *La norma de un producto es igual al producto de las normas, $N(\alpha\beta) = N(\alpha)N(\beta)$. $N(\alpha) = 0$ si y solamente si $\alpha = 0$. La norma de un entero en $R(\sqrt{m})$ es un entero racional. Si $\gamma$ es un entero en $R(\sqrt{m})$,* entonces *$N(\gamma) = \pm 1$ si y sólo si $\gamma$ es una unidad.*

*Demostración.* Para $\alpha$ y $\beta$ en $R(\sqrt{m})$ es fácil verificar que $\overline{(\alpha\beta)} = \bar{\alpha}\bar{\beta}$. Entonces se tiene $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\bar{\alpha}\beta\bar{\beta} = N(\alpha)N(\beta)$. Si $\alpha = 0$, entonces $\bar{\alpha} = 0$ y $N(\alpha) = 0$. Inversamente, si $N(\alpha) = 0$, entonces $\alpha\bar{\alpha} = 0$ de manera que $\alpha = 0$ o bien $\bar{\alpha} = 0$; pero $\bar{\alpha} = 0$ implica $\alpha = 0$.

A continuación, si $\gamma$ es un entero algebraico en $R(\sqrt{m})$, tiene grado 1 o bien 2. Si tiene grado 1, entonces, por el Teorema 9.9, $\gamma$ es un entero racional y $N(\gamma) = \gamma\bar{\gamma} = \gamma^2$ de manera que $N(\gamma)$ es un entero racional. Si $\gamma$ es de grado 2, entonces la ecuación mínima de $\gamma$, $x^2 - (\gamma + \bar{\gamma})x + \gamma\bar{\gamma} = 0$, tiene coeficientes enteros racionales y, nuevamente, $N(\gamma) = \gamma\bar{\gamma}$ es un entero racional.

Si $N(\gamma) = \pm 1$ y $\gamma$ es un entero, entonces $\gamma\bar{\gamma} = \pm 1$, $\gamma | 1$, de manera que $\gamma$ es una unidad. Para probar el inverso sea $\gamma$ una unidad. Entonces existe un entero $\varepsilon$ tal que $\gamma\varepsilon = 1$. Esto implica $N(\gamma)N(\varepsilon) = N(1) = 1$, de manera que $N(\gamma) = \pm 1$ ya que $N(\gamma)$ y $N(\varepsilon)$ son enteros racionales.

*Observación.* Con frecuencia, los enteros de $R(i)$ reciben el nombre de enteros gaussianos.

**Problemas**

1. Si un entero $\alpha$ en $R(\sqrt{m})$ no es cero ni una unidad, probar que $|N(\alpha)| > 1$.
2. Si $m \equiv 1 \pmod 4$, probar que los enteros de $R(\sqrt{m})$ son todos los números de la forma

$$a + b\,\frac{1 + \sqrt{m}}{2},$$

donde $a$ y $b$ son enteros racionales.

3. Si $\alpha$ es cualquier entero y $\varepsilon$ cualquier unidad, en $R(\sqrt{m})$, probar que $\varepsilon|\alpha$.
4. Si $\alpha$ y $\beta \neq 0$ son enteros en $R(\sqrt{m})$ y si $\alpha|\beta$, probar que $\bar{\alpha}|\bar{\beta}$ y $N(\alpha)|N(\beta)$.
5. Si $\alpha$ es un número algebraico en $R(\sqrt{m})$ con $m < 0$, probar que $N(\alpha) \geqq 0$. Demostrar que esto es falso si $m > 0$.
6. Probar que la siguiente aseveración es falsa en $R(i)$: Si $N(\alpha)$ es un entero racional, entonces $\alpha$ es un entero algebraico.
7. Probar que la aseveración del problema precedente es falsa en todo campo cuadrático. *Sugerencia*: Definir $\alpha = (x - 2\sqrt{m})/y$ de manera que $N(\alpha)$ es evidentemente un entero si $x$ y $y$ satisfacen $x^2 - y^2 = 4m$. Escoger $x = m + 1$, $y = m - 1$ de modo que $\alpha$ no es un entero si $|m - 1| > 4$. Los casos $|m - 1| \leqq 4$ pueden tratarse especialmente.

## 9.6 Unidades en los campos cuadráticos

Un campo cuadrático $R(\sqrt{m})$ se llama imaginario si $m < 0$ y se llama real si $m > 1$. Existen diferencias sorprendentes entre estos dos tipos de campos cuadráticos. Se verá que un campo cuadrático imaginario tiene sólo un número finito de unidades; de hecho para la mayoría de estos campos $\pm 1$ son las únicas unidades. Por otra parte, todo campo cuadrático real tiene un número infinito de unidades.

**Teorema 9.22** *Sea $m$ un entero racional negativo exento de cuadrados. El campo $R(\sqrt{m})$ tiene las unidades $\pm 1$, y éstas son las únicas unidades excepto en los casos $m = -1$ y $m = -3$. Las unidades para $R(i)$ son $\pm 1$ y $\pm i$. Las unidades para $R(\sqrt{-3})$ son $\pm 1$, $(1 \pm \sqrt{-3})/2$ y $(-1 \pm \sqrt{-3})/2$.*

*Demostración.* Tomando nota del Teorema 9.21, se buscan todos los enteros $\alpha$ en $R(\sqrt{m})$ tales que $N(\alpha) = \pm 1$. De acuerdo con el Teorema 9.20 puede escribirse $\alpha$ en una de las dos formas $x + y\sqrt{m}$ y $(x + y\sqrt{m})/2$ donde $x$ y $y$ son enteros racionales y donde, en la segunda forma, $x$ y $y$ son impares y $m \equiv 1 \pmod 4$. Entonces $N(\alpha) = x^2 - my^2$ o bien $N(\alpha) = (x^2 - my^2)/4$, respectivamente. Supuesto que $m$ es negativo se tiene $x^2 - my^2 \geqq 0$ de modo que no existe $\alpha$ con $N(\alpha) = -1$. Para $m < -1$ se tiene $x^2 - my^2 \geqq -my^2 \geqq 2y^2$ y las únicas soluciones de $x^2 - my^2 = 1$ son $y = 0$, $x = \pm 1$, en este caso. Para $m = -1$, la ecuación $x^2 - my^2 = 1$ tiene las soluciones $x = 0$, $y = \pm 1$, y $x = \pm 1$, $y = 0$ y no otras. Para $m \equiv 1 \pmod 4$, $m < -3$ no existen soluciones de $(x^2 - my^2)/4 = 1$ con $x$ y $y$ impares dado que $x^2 - my^2 \geqq 1 - m > 4$. Finalmente, para $m = -3$ se ve que las soluciones de la ecuación $(x^2 + 3y^2)/4 = 1$ con $x$ y $y$ impares son precisamente $x = 1$, $y = \pm 1$ y $x = -1$, $y = \pm 1$. Estas soluciones dan exactamente las unidades descritas en el teorema.

**Teorema 9.23** *Existe un número infinito de unidades en todo campo cuadrático real.*

*Demostración.* Los números $\alpha = x + y\sqrt{m}$ con enteros $x$, $y$ son enteros en $R(\sqrt{m})$ con normas $N(\alpha) = x^2 - my^2$. Si $x^2 - my = 1$, entonces $\alpha$ es una unidad. Pero la ecuación $x^2 - my^2 = 1$, $m > 1$ se trató en los Teoremas 7.25 y 7.26 donde se probó que tiene un número infinito de soluciones.

**Problema**

1. Probar que las unidades de $R(\sqrt{2})$ son $\pm(1 + \sqrt{2})^n$ donde $n$ recorre todos los enteros.

## 9.7 Los primos en los campos cuadráticos

**Definición 9.9** *Un entero algebraico $\alpha$, no una unidad, en un campo cuadrático $R(\sqrt{m})$ recibe el nombre de primo si sólo es divisible entre sus asociados y las unidades del campo.*

Esta definición es casi la misma que la definición de los primos entre los enteros racionales. No obstante, existe esta diferencia. En $R$

todos los primos son positivos, mientras que en $R(\sqrt{m})$ no se requiere tal propiedad. Así que si $\pi$ es un primo y $\varepsilon$ es una unidad en $R(\sqrt{m})$, entonces $\varepsilon\pi$ es un primo asociado en $R(\sqrt{m})$. Por ejemplo, $-\pi$ es un primo asociado de $\pi$.

**Teorema 9.24** *Si la norma de un entero $\alpha$ en $R(\sqrt{m})$ es $\pm p$, donde $p$ es un primo racional, entonces $\alpha$ es primo.*

*Demostración.* Supóngase que $\alpha = \beta\gamma$ donde $\beta$ y $\gamma$ son enteros en $R(\sqrt{m})$. Por el Teorema 9.21 se tiene $N(\alpha) = N(\beta)N(\gamma) = \pm p$. Entonces, dado que $N(\beta)$ y $N(\gamma)$ son enteros racionales, uno de ellos debe ser $\pm 1$, entonces ya sea $\beta$ o bien $\gamma$ es una unidad y el otro un asociado de $\alpha$. De donde $\alpha$ es primo.

**Teorema 9.25** *Todo entero en $R(\sqrt{m})$, que no sea cero o bien unidad, puede factorizarse en un producto de primos.*

*Demostración.* Si $\alpha$ no es primo, puede factorizarse en un producto $\beta\gamma$ donde ni $\beta$ ni $\gamma$ es una unidad. Repitiendo el procedimiento, se factoriza $\beta$ y $\gamma$ si no son primos. El proceso de factorización debe terminar puesto que de otra manera podría tenerse $\alpha$ en la forma $\beta_1\beta_2 \cdots \beta_n$ con $n$ arbitrariamente grande y ningún factor $\beta_j$ es unidad. Pero esto implicaría que

$$N(\alpha) = \prod_{j=1}^{n} N(\beta_j), \quad |N(\alpha)| = \prod_{j=1}^{n} |N(\beta_j)| \geqq 2^n, \quad n \text{ arbitraria,}$$

puesto que $|N(\beta_j)|$ es un entero $> 1$.

Aunque se ha establecido que hay factorización en primos, esta factorización no puede ser única. En efecto, se ha demostrado en la Sección 1.3 que la factorización en el campo $R(\sqrt{-6})$ no es única. En la sección siguiente se probará que la factorización es única en el campo $R(i)$. La cuestión general de los valores de $m$ para los cuales $R(\sqrt{m})$ tiene la propiedad de la factorización única es un problema no resuelto. Sin embargo, hay una íntima relación entre la factorización única y el algoritmo euclidiano, tal y como se demostrará ahora.

Precisamente como en el caso del campo racional, un teorema de factorización única tendrá que pasar por alto el orden en el cual aparecen los diversos factores primos. Pero ahora se presenta una nueva ambigüedad debido a la existencia de los primos asociados. Las dos factorizaciones

$$\alpha = \pi_1\pi_2 \cdots \pi_r = (\varepsilon_1\pi_1)(\varepsilon_2\pi_2) \cdots (\varepsilon_r\pi_r)$$

donde los $\varepsilon_j$ son unidades con producto 1, tendrán que considerarse como las mismas.

**Definición 9.10** *Se dice que un campo cuadrático* $R(\sqrt{m})$ *tiene la propiedad de la factorización única si todo entero* $\alpha$ *en* $R(\sqrt{m})$; que *no sea cero o bien unidad, puede factorizarse unívocamente en primos, independientemente del orden de los primos y de las ambigüedades entre los primos asociados.*

**Definición 9.11** *Se dice que un campo cuadrático* $R(\sqrt{m})$ *es euclidiano si los enteros* $R(\sqrt{m})$ *satisfacen un algoritmo euclidiano, esto es, si* $\alpha$ *y* $\beta$ *son enteros de* $R(\sqrt{m})$ *con* $\beta \neq 0$, *existen los enteros* $\gamma$ *y* $\delta$ *de* $R(\sqrt{m})$ *tales que* $\alpha = \beta\gamma + \delta$, $|N(\delta)| < |N(\beta)|$.

**Teorema 9.26** *Todo campo cuadrático euclidiano tiene la propiedad de la factorización única.*

*Demostración.* La demostración de este teorema es semejante al procedimiento aplicado al establecer el teorema fundamental de la aritmética, Teorema 1.16. Primero se establece que si $\alpha$ y $\beta$ son dos enteros cualesquiera de $R(\sqrt{m})$ que no tienen factores comunes excepto unidades, entonces existen los enteros $\lambda_0$ y $\mu_0$ en $R(\sqrt{m})$ tales que $\alpha\lambda_0 + \beta\mu_0 = 1$. Denotemos por $S$ el conjunto de enteros de la forma $\alpha\lambda + \beta\mu$ donde $\lambda$ y $\mu$ recorren todos los enteros de $R(\sqrt{m})$. La norma $N(\alpha\lambda + \beta\mu)$ de cualquier entero en $S$ es un entero racional, de modo que puede escogerse un entero digamos $\alpha\lambda_1 + \beta\mu_1 = \varepsilon$, tal que $|N(\varepsilon)|$ es el menor valor positivo tomado por $|N(\alpha\lambda + \beta\mu)|$. Aplicando el algoritmo euclidiano a $\alpha$ y $\varepsilon$ se obtiene

$$\alpha = \varepsilon\gamma + \delta, \quad |N(\delta)| < |N(\varepsilon)|.$$

Entonces se tiene

$$\delta = \alpha - \varepsilon\gamma = \alpha - \gamma(\alpha\lambda_1 + \beta\mu_1) = \alpha(1 - \gamma\lambda_1) + \beta(-\gamma\mu_1)$$

de modo que $\delta$ es un entero en $S$. Ahora esto requiere $|N(\delta)| = 0$ por la definición de $\varepsilon$ y, por el Teorema 9.21, se tiene $\delta = 0$. Así que $\alpha = \varepsilon\gamma$ de donde $\varepsilon|\alpha$. De modo semejante, se encuentra $\varepsilon|\beta$ y, por tanto, $\varepsilon$ es unidad. Entonces por el Teorema 9.19, $\varepsilon^{-1}$ también es unidad, y se tiene, digamos

$$1 = \varepsilon^{-1}\varepsilon = \varepsilon^{-1}(\alpha\lambda_1 + \beta\mu_1) = \alpha(\varepsilon^{-1}\lambda_1) + \beta(\varepsilon^{-1}\mu_1) = \alpha\lambda_0 + \beta\mu_0,$$

A continuación se probará que si $\pi$ es primo en $R(\sqrt{m})$ y si $\pi|\alpha\beta$, entonces $\pi|\alpha$ o bien $\pi|\beta$. Porque si $\pi \nmid \alpha$, entonces $\pi$ y $\alpha$ no tienen factores comunes excepto unidades y, existen los enteros $\lambda_0$ y $\mu_0$ tales que $1 = \pi\lambda_0 + \alpha\mu_0$. Entonces $\beta = \pi\beta\lambda_0 + \alpha\beta\mu_0$ y $\pi|\beta$ debido a que $\pi|\alpha\beta$. Esto

puede extenderse por inducción matemática para probar que si $\pi|(\alpha_1 \alpha_2 \cdots \alpha_n)$, entonces $\pi$ divide por lo menos a un factor $\alpha_j$ del producto.

A partir de este punto, la demostración es idéntica a la primera demostración del Teorema 1.16 y no es necesario repetir los detalles.

**Problemas**

1. Si $\pi$ es primo y $\varepsilon$ es unidad en $R(\sqrt{m})$, probar que $\varepsilon\pi$ es primo.
2. Probar que $1 + i$ es un primo en $R(i)$.
3. Probar que $11 + 2\sqrt{6}$ es un primo en $R(\sqrt{6})$.
4. Probar que 3 es un primo en $R(i)$ pero no es un primo en $R(\sqrt{6})$
5. Probar que existe un número infinito de primos en todo campo cuadrático $R(\sqrt{m})$.

## 9.8 Factorización única

En esta sección se aplicará el Teorema 9.26 a varios campos cuadráticos, a saber $R(i)$, $R(\sqrt{-2})$; $R(\sqrt{-3})$, $R(\sqrt{-7})$, $R(\sqrt{2})$, $R(\sqrt{3})$. Se demostrará que estos campos tienen la propiedad de la factorización única probando que son campos euclidianos. Existen otros campos cuadráticos euclidianos pero enfocaremos nuestra atención en estos campos para los cuales el algoritmo euclidiano se establece fácilmente.

**Teorema 9.27** *Los campos $R(\sqrt{m})$ para $m = -1, -2, -3, -7$, 2, 3, son euclidianos y, por tanto, tienen la propiedad de la factorización única.*

*Demostración.* Considérense cualesquiera enteros $\alpha$ y $\beta$ de $R(\sqrt{m})$ con $\beta \neq 0$. Entonces $\alpha/\beta = u + v\sqrt{m}$ donde $u$ y $v$ son números racionales y se escogen los enteros racionales $x$ y $y$ que estén más próximos a $u$ y $v$, esto es, de manera que

$$(9.10) \qquad 0 \leqq |u - x| \leqq \tfrac{1}{2}, \qquad 0 \leqq |v - y| \leqq \tfrac{1}{2}.$$

Si se denota $x + y\sqrt{m}$ por $\gamma$ y $\alpha - \beta\gamma$ por $\delta$, entonces $\gamma$ y $\delta$ son enteros en $R(\sqrt{m})$ y $N(\delta) = N(\alpha - \beta\gamma) = N(\beta)N(\alpha/\beta - \gamma) = N(\beta)N((u - x) + (v - y)\sqrt{m}) = N(\beta)\{(u - x)^2 - m(v - y)^2\}$,

$$(9.11) \qquad |N(\delta)| = |N(\beta)|\,|(u - x)^2 - m(v - y)^2|.$$

Por las ecuaciones (9.10) se tiene

$$-\frac{m}{4} \leqq (u - x)^2 - m(v - y)^2 \leqq \frac{1}{4} \quad \text{si} \quad m > 0,$$

$$0 \leqq (u - x)^2 - m(v - y)^2 \leqq \frac{1}{4} + \frac{1}{4}(-m) \quad \text{si} \quad m < 0,$$

y de aquí que, por (9.11), $|N(\delta)| < |N(\beta)|$ si $m = 2, 3, -1, -2$. Por lo tanto, $R(\sqrt{m})$ es euclidiano para estos valores de $m$.

Para los casos $m = -3$ y $m = -7$ debe escogerse $\gamma$ en una forma diferente. Con $u$ y $v$ definidos como antes, se escoge un entero racional $s$ tan próximo a $2v$ como sea posible y entonces se escoge un entero racional $r$, tal que $r \equiv s \pmod 2$, tan próximo a $2u$ como sea posible. Entonces se tiene $|2v - s| \leqq \frac{1}{2}$ y $|2u - r| \leqq 1$, y el número $\gamma = (r + s\sqrt{m})/2$ es un entero de $R(\sqrt{m})$ por el Teorema 9.20, puesto que $m \equiv 1 \pmod 4$ en los casos bajo discusión. Como antes, $\delta = \alpha - \beta\gamma$ es un entero en $R(\sqrt{m})$ y

$$N(\delta) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) = N(\beta)\left\{\left(u - \frac{r}{2}\right)^2 - m\left(v - \frac{s}{2}\right)^2\right\},$$

$$|N(\delta)| \leqq |N(\beta)|\left\{\frac{1}{4} + \frac{1}{16}(-m)\right\} < |N(\beta)|,$$

para $m = -3$ y $m = -7$.

**Problemas**

1. Probar que $R(\sqrt{-11})$ tiene la propiedad de la factorización única.
2. Probar que $R(\sqrt{5})$ tiene la propiedad de la factorización única.
3. Probar que en $R(i)$ el cociente $\gamma$ y el residuo $\delta$ obtenidos en la demostración del Teorema 9.27 no son necesariamente únicos. Esto es, probar que en $R(i)$ existen los enteros $\alpha$, $\beta$, $\gamma$, $\delta$, $\gamma_1$, $\delta_1$ tales que

$$\alpha = \beta\gamma + \delta = \beta\gamma_1 + \delta_1, \quad N(\delta) < N(\beta), \quad N(\delta_1) < N(\beta), \quad \gamma \neq \gamma_1, \quad \delta \neq \delta_1$$

4. Si $\alpha$ y $\beta$ son enteros de $R(i)$, no ambos cero, digamos que $\gamma$ es un máximo común divisor de $\alpha$ y $\beta$ si $N(\gamma)$ es máximo entre las normas de todos los divisores comunes de $\alpha$ y $\beta$. Probar que existen exactamente cuatro máximos comunes divisores de toda pareja fija $\alpha$, $\beta$ y que cada uno de los cuatro es divisible entre cualquier divisor común.

## 9.9 Primos en los campos cuadráticos que tienen la propiedad de la factorización única

Si un campo $R(\sqrt{m})$ tiene la propiedad de la factorización única, puede decirse mucho más acerca de las primos del campo que lo que se dijo en la Sección 9.7.

**Teorema 9.28** *Supóngase que $R(\sqrt{m})$ tiene la propiedad de la factorización única. Entonces a todo primo $\pi$ en $R(\sqrt{m})$ le corresponde uno y solamente un primo racional $p$ tal que $\pi | p$.*

*Demostración.* El primo $\pi$ es un divisor del entero racional $N(\pi)$ y de aquí que existan los enteros racionales positivos divisibles entre $\pi$. Sea $n$ el menor de éstos. Entonces $n$ es un primo racional, porque de otra manera $n = n_1 n_2$, y se tiene, por la propiedad de la factorización única, $\pi|n$, $\pi|(n_1 n_2)$, $\pi|n_1$ o bien $\pi|n_2$, una contradicción puesto que $0 < n_1 < n$, $0 < n_2 < n$. De donde $n$ es un primo racional, llamémosle $p$. Y, si $\pi$ fuera un divisor de otro primo racional $q$, por el Teorema 1.3, podrían encontrarse los enteros racionales tales que $1 = px + qy$. Ya que $\pi|(px + qy)$ esto implica $\pi|1$, lo cual es falso, y de aquí que el primo $p$ es único.

**Teorema 9.29** *Supongamos que $R(\sqrt{m})$ tiene la propiedad de la factorización única. Entonces:*

1) *Cualquier primo racional $p$ es un primo $\pi$ del campo o bien un producto $\pi_1\pi_2$ de dos primos, no necesariamente distintos, de $R(\sqrt{m})$.*
2) *La totalidad de los primos $\pi, \pi_1; \pi_2$ obtenidos aplicando la parte 1 a todos los primos racionales, junto con sus asociados, constituyen el conjunto de todos los primos de $R(\sqrt{m})$.*
3) *Un primo racional impar $p$ que satisface $(p, m) = 1$ es un producto $\pi_1\pi_2$ de dos primos en $R(\sqrt{m})$ si, y sólo si, $\left(\frac{m}{p}\right) = 1$.*
4) *Si $(2, m) = 1$, entonces 2 es el asociado de un cuadrado de un primo si $m \equiv 3 \pmod 4$; 2 es un primo si $m \equiv 5 \pmod 8$; y 2 es el producto de dos primos distintos si $m \equiv 1 \pmod 8$.*
5) *Todo primo racional $p$ que divide a $m$ es el asociado del cuadrado de un primo en $R(\sqrt{m})$.*

*Demostración.* 1) Si el primo racional $p$ no es primo en $R(\sqrt{m})$, entonces $p = \pi\beta$ para algún primo $\pi$ y algún entero $\beta$ de $R(\sqrt{m})$. Entonces se tiene $N(\pi)N(\beta) = N(p) = p^2$. Dado que $N(\pi) \neq \pm 1$, debe tenerse $N(\beta) = \pm 1$ o bien $N(\beta) = \pm p$. Si $N(\beta) = \pm 1$, entonces, por el Teorema 9.21, $\beta$ es una unidad y $\pi$ es un asociado de $p$, el cual entonces debe ser primo en $R(\sqrt{m})$. Si $N(\beta) = \pm p$ debe demostrarse que $\beta$ es primo. Si $\beta = \beta_1\beta_2$, entonces $N(\beta_1)N(\beta_2) = \pm p$ y uno de $N(\beta_1)$ y $N(\beta_2)$ debe tener el valor $\pm 1$, de modo que $\beta_1$ o bien $\beta_2$ es una unidad. De donde $\beta$ es primo y $p$ es un producto $\pi\beta$ de dos primos en $R(\sqrt{m})$.

2) La proposición 2) ahora se concluye directamente del Teorema 9.28 y la proposición 1).

3) Si $p$ es un primo racional impar tal que $(p, m) = 1$ y $\left(\frac{m}{p}\right) = 1$, existe un entero racional $x$ que satisface

$$x^2 \equiv m \pmod p, \quad p|(x^2 - m), \quad p|(x - \sqrt{m})(x + \sqrt{m}).$$

Si $p$ fuera primo de $R(\sqrt{m})$, dividiría uno de los factores $x - \sqrt{m}$ y $x + \sqrt{m}$, de manera que uno de

$$\frac{x}{p} - \frac{\sqrt{m}}{p}, \qquad \frac{x}{p} + \frac{\sqrt{m}}{p}$$

sería un entero en $R(\sqrt{m})$. Pero, por el Teorema 9.20, esto es imposible y de donde $p$ no es primo en $R(\sqrt{m})$. Por tanto, por la proposición 1), $p = \pi_1\pi_2$ *si* $\left(\frac{m}{p}\right) = 1$.

Ahora supóngase que $p$ es un primo racional impar, que $(p, m) = 1$ y que $p$ no es un primo en $R(\sqrt{m})$. Entonces, a partir de la demostración de la proposición 1) se ve que $p = \pi\beta$, $N(\beta) = \pm p$ y $N(\pi) = \pm p$. Puede escribirse $\pi = a + b\sqrt{m}$ donde $a$ y $b$ son enteros racionales o bien, si $m \equiv 1 \pmod 4$, mitades de enteros racionales impares. Entonces $a^2 - mb^2 = N(\pi) = \pm p$ y se tiene $(2a)^2 - m(2b)^2 = \pm 4p$, $(2a)^2 \equiv m(2b)^2 \pmod p$. Aquí $2a$ y $2b$ son enteros racionales y ninguno es múltiplo de $p$, porque si $p$ dividiera a uno, dividiría al otro y se tendría $p^2|4a^2$, $p^2|4b^2$, $p^2|(4a^2 - 4mb^2)$, $p^2|4p$. Por lo tanto, $(2b, p) = 1$ y existe un entero racional $w$ tal que $2bw \equiv 1 \pmod p$, $(2aw)^2 \equiv m(2bw)^2 \equiv m \pmod p$, y se tiene $\left(\frac{m}{p}\right) = 1$.

4) Si $m \equiv 3 \pmod 4$, entonces

$$m^2 - m = 2\frac{m^2 - m}{2} = (m + \sqrt{m})(m - \sqrt{m}),$$

y $2 \nmid (m \pm \sqrt{m})$, de manera que 2 no puede ser un primo de $R(\sqrt{m})$. De donde 2 es divisible por un primo $x + y\sqrt{m}$ y este primo debe tener norma $\pm 2$. Por tanto, $x^2 - my^2 = \pm 2$. Pero éste implica que

$$\pm\frac{x - y\sqrt{m}}{x + y\sqrt{m}} = \pm\frac{x^2 + my^2 - 2xy\sqrt{m}}{x^2 - my^2} = \frac{x^2 + my^2}{2} - xy\sqrt{m},$$

y, de modo semejante,

$$\pm\frac{x + y\sqrt{m}}{x - y\sqrt{m}} = \frac{x^2 + my^2}{2} + xy\sqrt{m},$$

y, por lo tanto $(x - y\sqrt{m})(x + y\sqrt{m})^{-1}$ y su inverso son los enteros de $R(\sqrt{m})$. De donde $(x - y\sqrt{m})(x + y\sqrt{m})^{-1}$ es una unidad y $x - y\sqrt{m}$ y $x + y\sqrt{m}$ son asociados.

Si $m \equiv 1 \pmod 4$ y si 2 no es un primo en $R(\sqrt{m})$ entonces 2 es divisible entre un primo $\frac{1}{2}(x + y\sqrt{m})$ que tiene la norma $\pm 2$. Esto significaría que existen los enteros racionales $x$ y $y$, ambos pares o bien impares tales que

$$(9.12) \qquad x^2 - my^2 = \pm 8.$$

Si $x$ y $y$ son pares, digamos $x = 2x_0$, $y = 2y_0$, entonces (9.12) requeriría $x_0^2 - my_0^2 = \pm 2$. Pero, puesto que $m \equiv 1 \pmod 4$, $x_0^2 - my_0^2$ es impar o bien múltiplo de 4. Así que (9.12) puede tener soluciones sólo con $x$ y $y$ impares. Entonces $x^2 \equiv y^2 \equiv 1 \pmod 8$ y (9.12) implica que

$$x^2 - my^2 \equiv 1 - m \equiv 0, \qquad m \equiv 1 \pmod 8.$$

Se concluye que 2 es un primo en $R(\sqrt{m})$ si $m \equiv 5 \pmod 8$.

Ahora bien, si $m \equiv 1 \pmod 8$ se observa que

$$\frac{1-m}{4} = 2\frac{1-m}{8} = \frac{1-\sqrt{m}}{2}\,\frac{1+\sqrt{m}}{2},$$

y $2 \nmid (1 \pm \sqrt{m})/2$, de modo que 2 no puede ser un primo en $R(\sqrt{m})$. De donde (9.12) tiene soluciones en los enteros impares $x$ y $y$. Ahora bien, los primos $\frac{1}{2}(x + y\sqrt{m})$ y $\frac{1}{2}(x - y\sqrt{m})$ no son asociados en $R(\sqrt{m})$ debido a que su cociente no es una unidad. De hecho su cociente es

$$\frac{x + y\sqrt{m}}{x - y\sqrt{m}} = \pm\frac{x^2 + my^2}{8} \pm \frac{xy\sqrt{m}}{4}$$

lo cual incluso no es un entero en $R(\sqrt{m})$.

5) Sea $p$ un divisor primo racional de $m$. Si $p = |m|$ entonces $p = \pm\sqrt{m}\cdot\sqrt{m}$ y de aquí que $p$ es el asociado del cuadrado de un primo en $R(\sqrt{m})$. *Si* $p < |m|$ se observa que

$$(9.13) \qquad m = p\frac{m}{p} = \sqrt{m}\cdot\sqrt{m}.$$

Pero $p$ no es un divisor de $\sqrt{m}$ en $R(\sqrt{m})$ y de aquí que $p$ no es un primo en $R(\sqrt{m})$. Por tanto $p$ es divisible entre un primo $\pi$, con $N(\pi) = \pm p$ y de donde no es un divisor de $m/p$. Pero, por (9.13), $\pi$ también es un divisor de $\sqrt{m}$, $\pi^2$ es un divisor de $m$ y; por tanto, $\pi^2$ es un divisor de $p$.

El teorema que acaba de probarse proporciona un método para determinar los primos de un campo cuadrático que tiene la propiedad de la factorización única. Para tal $R(\sqrt{m})$ se buscan todos los primos racionales $p$. Aquellos $p$ para los cuales $(p, 2m) = 1$ y $\left(\frac{m}{p}\right) = -1$,

junto con todos sus asociados en $R(\sqrt{m})$, son primos en $R(\sqrt{m})$. Aquellos $p$ para los cuales $(p, 2m) = 1$ y $\left(\frac{m}{p}\right) = +1$ se factorizarán en $p = \pi_1\pi_2$, un producto de dos primos de $R(\sqrt{m})$, con $N(\pi_1) = N(\pi_2) = \pm p$. Cualquier otra factorización de $p$ simplemente reemplazará $\pi_1$ y $\pi_2$ por los asociados. Los primos $p$ para los cuales $(p, 2m) > 1$ serán primos de $R(\sqrt{m})$ o bien productos de dos primos de $R(\sqrt{m})$.

Supóngase que $\alpha$ es un entero en $R(\sqrt{m})$ y que $N(\alpha) = \pm p$, $p$ un primo racional. Entonces $\alpha$ también es un entero en $R(\sqrt{m})$ y $\alpha\bar{\alpha} = N(\alpha) = \pm p$, y esto necesita que $\alpha$ sea un primo en $R(\sqrt{m})$. Si $m \not\equiv 1 \pmod 4$, puede escribirse $\alpha = x + y\sqrt{m}$, $N(\alpha) = x^2 - my^2$, con los enteros $x$ y $y$. Si $m \equiv 1 \pmod 4$, puede escribirse $\alpha = (x + y\sqrt{m})/2$, $4N(\alpha) = x^2 - my^2$, *con* $x$ y $y$ enteros, ambos impares o bien ambos pares.

Combinando estos hechos se tiene lo siguiente. Supóngase que $R(\sqrt{m})$ tiene la propiedad de la factorización única, y sea $p$ un primo racional tal que $(p, 2m) = 1$, $\left(\frac{m}{p}\right) = +1$. Entonces, si $m \not\equiv 1 \pmod 4$, por lo menos una de las dos ecuaciones $x^2 - my^2 = \pm p$ tiene una solución. Sea $x = a$, $y = b$ esa solución. Entonces los números $\alpha = a + b\sqrt{m}$, $\bar{\alpha} = a - b\sqrt{m}$ y los asociados de $\alpha$ y $\bar{\alpha}$ son primos en $R(\sqrt{m})$ y éstos son los únicos primos en $R(\sqrt{m})$ que dividen a $p$. Por otra parte, si $m \equiv 1 \pmod 4$, por lo menos una de las dos ecuaciones $x^2 - my^2 = \pm 4p$ tiene una solución con $x$ y $y$ ambos impares o bien ambos pares. Denotando otra vez esa solución por $x = a$, $y = b$, puede decirse que los números $\alpha = (a + b\sqrt{m})/2$, $\bar{\alpha} = (a - b\sqrt{m})/2$ y sus asociados son primos en $R(\sqrt{m})$ y éstos son los únicos primos en $R(\sqrt{m})$ que dividen a $p$. Merece hacerse notar que nuestra consideración de los campos de números algebraicos así nos han proporcionado información referente a las ecuaciones diofantinas.

Debe recordarse que estos resultados se aplican únicamente a aquellos $R(\sqrt{m})$ que tienen la propiedad de la factorización única.

**Ejemplo.** $m = -1$. Primos gaussianos. El campo es $R(i)$ y se tiene

$$2m = -2, \quad 1^2 + 1^2 = 2, \quad \overline{1 + i} = 1 - i,$$

$$\left(\frac{m}{p}\right) = \begin{cases} +1 & \text{si } p = 4k + 1 \\ -1 & \text{si } p = 4k + 3. \end{cases}$$

Para cada primo racional $p$ de la forma $4k + 1$, la ecuación $x^2 + y^2 = p$ tiene una solución puesto que $x^2 + y^2 = -p$ evidentemente es imposible. Para esa $p$ se escoge una solución $x = a_p$, $y = b_p$.

Los primos en $R(i)$ son $1+i$, todos los primos racionales $p=4k+3$, todos los $a_p+ib_p$, todos los $a_p-ib_p$, junto con todos sus asociados. Obsérvese que $1-i=\overline{1+i}$ no ha sido incluido puesto que $1-i=-i(1+i)$, $i$ es una unidad de $R(i)$ y de aquí que $1-i$ es un asociado $1+i$.

**Ejemplo.** $m=-3$. El campo es $R(\sqrt{-3})$ y se tiene

$$2m=-6. \quad x^2+3y^2=\pm 4\cdot 2 \text{ no tiene solución}$$

$$3^2+3\cdot 1^2=4\cdot 3, \quad \overline{\frac{3+\sqrt{-3}}{2}}=\frac{3-\sqrt{-3}}{2},$$

$$\left(\frac{m}{p}\right)=\begin{cases}+1 \text{ si } p=3k+1,\ (p,6)=1\\ -1 \text{ si } p=3k+2,\ (p,6)=1.\end{cases}$$

Para cada impar $p=3k+1$, se escoge $a_p$, $b_p$ tal que $a_p^2+3b_p^2=4p$.

Los primos en $R(\sqrt{-3})$ son 2, $(3+\sqrt{-3})/2$, todos los primos racionales impares $p=3k+2$, todos los $(a_p+b_p\sqrt{-3})/2$, todos los $(a_p-b_p\sqrt{-3})/2$, junto con todos sus asociados. Aquí, otra vez se omite $(3-\sqrt{-3})/2$ debido a que puede demostrarse que es un asociado de $(3+\sqrt{-3})/2$. Podría haberse incluido 2 entre los $p=3k+2$ únicamente omitiendo la palabra "impares".

Puede observarse que después de las secciones 9.1-9.4 sobre los números algebraicos en general, hemos vuelto nuestra atención a los campos cuadráticos. Muchos de los teoremas pueden extenderse hacia los campos de números algebraicos de grado superior pero, por supuesto, no es posible obtener los resultados tan detallados como para los campos cuadráticos. Nuestra breve exploración de los números algebraicos no sólo ha omitido estas generalizaciones sino también muchos otros aspectos de la teoría de los números algebraicos que se han investigado.

•

**Problemas**

1. En el segundo ejemplo, donde $m=-3$, se sabe, con base en la teoría, que si $p$ es cualquier primo de la forma $3k+1$, entonces existen los enteros $x$ y $y$ tales que $x^2+3y^2=4p$. Sea $x=2u-y$ y establecer que todo primo de ese tipo puede expresarse en la forma $u^2-uy+y^2$.
2. El primo racional 13 puede factorizarse en dos formas $R(\sqrt{-3})$,

$$13=\frac{7+\sqrt{-3}}{2}\cdot\frac{7-\sqrt{-3}}{2}=(1+2\sqrt{-3})(1-2\sqrt{-3}).$$

Probar que esto no está en conflicto con el hecho de que $R(\sqrt{-3})$ tiene la propiedad de la factorización única.

3. Probar que $\sqrt{3}-1$ y $\sqrt{3}+1$ son asociados en $R(\sqrt{3})$.
4. Probar que los primos de $R(\sqrt{3})$ son $\sqrt{3}-1$, $\sqrt{3}$ todos los primos racionales $p\equiv\pm 5 \pmod{12}$, todos los factores $a+b\sqrt{3}$ de los primos racionales $p\equiv\pm 1 \pmod{12}$ y todos los asociados de estos primos.

5. Probar que los primos de $R(\sqrt{2})$ son $\sqrt{2}$, todos los primos racionales de la forma $8k \pm 3$ y todos los factores $a + b\sqrt{2}$ de los primos racionales de la forma $8k \pm 1$ y todos los asociados de estos primos.
6. Probar que si $m$ es exento de cuadrados, $m < 0$, $|m|$ no primo, entonces $R(\sqrt{m})$ no tiene la propiedad de la factorización única. *Sugerencia*: aplicar la parte (5) del Teorema 9.29.

# Capítulo 10

# La función partición

## 10.1 Particiones

**Definición 10.1** *La función partición* $p(n)$ *se define como el número de maneras en que el entero positivo* $n$ *puede escribirse como una suma de enteros positivos. No se considera que dos particiones sean diferentes si difieren solamente en el orden de sus sumandos. Es conveniente definir* $p(0) = 1$.

Por ejemplo $5 = 5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$, y $p(5) = 7$. De modo semejante, $p(1) = 1, p(2) = 2$, $p(3) = 3$, $p(4) = 5$.

Pueden definirse otras funciones partición para las cuales los sumandos deben satisfacer ciertas restricciones. Haremos uso de algunas de éstas.

**Definición 10.2**

$p_m(n)$ = *el número de particiones de* $n$ *en sumandos menores que o bien iguales a* $m$.
$p^o(n)$ = *el número de particiones de* $n$ *en sumandos impares.*
$p^d(n)$ = *el número de particiones de* $n$ *en sumandos distintos.*
$q^e(n)$ = *el número de particiones de* $n$ *en un número par de sumandos distintos.*
$q^o(n)$ = *el número de particiones de* $n$ *en un número impar de sumandos distintos.*

*Haremos la convención* $p_m(0) = p^o(0) = p^d(0) = q^e(0) = 1$, $q^o(0) = 0$.

Dado que $5 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$, se tiene $p_2(5) = 3$. También $5 = 5 = 3 + 1 + 1 = 1 + 1 + 1 + 1 + 1$, y $5 = 5 = 4 + 1 = 3 + 2$, y $5 = 4 + 1 = 3 + 2$ y $5 = 5$, de manera que $p^o(5) = 3$, $p^d(5) = 3$, $q^e(5) = 2$, $q^o(5) = 1$.

**Teorema 10.1** *Se tiene*

*a*) $p_m(n) = p(n)$ *si* $n \leqq m$,
*b*) $p_m(n) \leqq p(n)$ *para todo* $n \geqq 0$,
*c*) $p_m(n) = p_{m-1}(n) + p_m(n - m)$ *si* $n \geqq m > 1$,
*d*) $p^d(n) = q^e(n) + q^o(n)$.

*Demostración.* Con la excepción posible de $(c)$, todas estas son obvias a partir de las definiciones. Para probar $(c)$ se observa que cada partición de $n$ contada por $p_m(n)$ tiene o bien no tiene un sumando igual a $m$. Las particiones de la segunda clase son contadas por $p_{m-1}(n)$. Las particiones de la primera clase se obtienen agregando un sumando $m$ a cada partición de $n - m$ en sumandos menores que o iguales a $m$, y de aquí que en número son $p_m(n - m)$. Si $n = m$, el término $p_m(n - m) = 1$ cuenta la sola partición $n = m$.

**Teorema 10.2** *Para* $n \geqq 1$ *se tiene* $p^d(n) = p^o(n)$.

*Demostración.* Considérese cualquier partición contada por $p^o(n)$. Consistirá, digamos, de $r_1$ sumandos $a_1$, $r_2$ sumandos $a_2, \ldots, r_s$, sumandos $a_s$, donde los $a_i$ son enteros impares distintos y $\sum_{i=1}^{s} r_i a_i = n$. Ahora puede escribirse cada $r_i$ en la forma $r_i = \sum_j b_j^{(i)} 2^j$, $b_j^{(i)} = 0$ o bien 1. Entonces $n = \sum_{i=1}^{s} \sum_j b_j^{(i)} 2^j a_i$ nos proporciona una partición de $n$ cuyos sumandos son todos los enteros $2^j a_i$ para los cuales $b_j^{(i)} = 1$.

También, supuesto que los $a_i$ son distintos e impares; los sumandos $2^j a_i$ son distintos, y esta nueva partición se cuenta por $p^d(n)$.

Puede invertirse el proceso. Si $n = \sum_{k=1}^{t} c_k$ y los $c_k$ son distintos, se escribe cada $c_k$ como $2^{e_k} d_k$, $d_k$ impar. Entonces supongamos que $a_1, a_2, \ldots, a_s$ son todos los enteros diferentes que deben encontrarse entre los $d_1, d_2, \ldots, d_t$ y supongamos que $b_j^{(i)} = 1$ si $2^j a_i$ es algún $c_k$, de otra manera $b_j^{(i)} = 0$. Entonces $\sum_{i=1}^{s} \sum_j b_j^{(i)} 2^i a_i = \sum_{k=1}^{t} c_k = n$ y se regresa a la partición de $n$ en $r_1$ sumandos $a_1$, $r_2$ sumandos $a_2, \ldots, r_s$ sumandos $a_s$ donde $r_i = \sum_j b_j^{(i)} 2^j$. Se ha encontrado una correspondencia biunívoca entre las particiones contadas por $p^o(n)$ y las contadas por $p^d(n)$ y de aquí que se tiene $p^o(n) = p^d(n)$.

## 10.2 Gráficas

Una partición de $n$ puede representarse geométricamente. Si $n = a_1 + a_2 + \cdots + a_r$ es una partición, pueden arreglarse los sumandos $a_i$ en tal forma que $a_1 \geqq a_2 \geqq \cdots \geqq a_r$. Entonces la gráfica de esta partición es el arreglo de puntos que tiene a los puntos $a_1$ en el renglón superior, los $a_2$ en el siguiente renglón y así sucesivamente hacia abajo hasta los $a_r$ en el renglón inferior.

$$
\begin{array}{llllll}
\bullet & \bullet & \bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \bullet & \bullet & \\
\bullet & \bullet & \bullet & \bullet & \bullet & \\
\bullet & \bullet & & & & \\
\bullet & & & & &
\end{array}
$$

$$19 = 6 + 5 + 5 + 2 + 1.$$

Si se lee la gráfica verticalmente en lugar de horizontalmente, se obtiene una partición posiblemente diferente. Por ejemplo, de $19 = 6 + 5 + 5 + 2 + 1$ se obtiene $19 = 5 + 4 + 3 + 3 + 3 + 1$. A partir de la partición $n = a_1 + a_2 + \cdots + a_r$ que consiste de $r$ sumandos con el mayor sumando $a_1$, se obtiene una partición de $n$ en $a_1$ sumandos con el mayor sumando $r$. Dado que esta correspondencia es reversible se tiene el siguiente teorema.

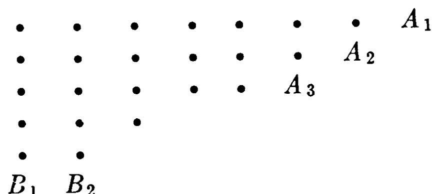
**Teorema 10.3** *El número de particiones de $n$ en $m$ sumandos es el mismo que el número de particiones de $n$ que tiene el mayor sumando $m$. El número de particiones de $n$ en cuando más $m$ sumandos es $p_m(n)$.*

**Teorema 10.4** *Si $n \geqq 0$ entonces*

$$q^e(n) - q^o(n) = \begin{cases} (-1)^j & \text{si } n = (3j^2 \pm j)/2 \textit{ para algún } j = 0, 1, 2, \cdots \\ 0 & \textit{en cualquier otro caso.} \end{cases}$$

*Demostración.* Para $n = 0$ se tiene $j = 0$ y $q^e(0) - q^o(0) = 1$. Ahora supóngase que $n \geqq 1$ y considérese una partición $n = a_1 + a_2 + \cdots + a_r$ en sumandos distintos. En la gráfica de esta partición; denotemos por $A_1$ el punto más alejado a la derecha del primer renglón. Supuesto que los sumandos son distintos, no habrá punto directamente abajo de $A_1$. Si $a_2 = a_1 - 1$, habrá un punto $A_2$ directamente abajo del punto que está inmediatamente a la izquierda de $A_1$. Si $a_2 < a_1 - 1$, no habrá tal punto $A_2$. Si $a_3 = a_1 - 2$, entonces $a_2 = a_1 - 1$ y habrá un punto $A_3$ directamente abajo del punto que está inmediatamente a la izquierda de $A_2$. Si $a_2 = a_1 - 1$ y $a_3 < a_2 - 1$, no habrá punto $A_3$. Se continúa este proceso hasta donde sea posible, obteniendo así un conjunto de puntos $A_1, A_2, \ldots, A_s$, $s \geqq 1$, que se encuentran en una

línea que pasa por $A_1$ con pendiente 1. También designemos los puntos del renglón inferior por $B_1, B_2, \ldots, B_t$, $t = a_r$. Nótese que $B_t$ y $A_s$ pueden ser el mismo punto.




Ahora se desea cambiar la gráfica en la gráfica de otra partición de $n$ en sumandos distintos. Primero, tratemos de tomar los puntos $B_1, B_2, \ldots, B_t$ y colocarlos a la derecha de $A_1, A_2, \ldots, A_t$; $B_1$ a la derecha de $A_1$, $B_2$ a la derecha de $A_2$, etc. Es obvio que no puede hacerse esto si $t > s$ o bien si $t = s$ y $B_t = A_s$. Sin embargo, puede hacerse si $t < s$ o bien si $t = s$ y $B_t \neq A_s$, y se obtiene una gráfica de una partición en sumandos distintos. Segundo, tratemos de invertir el proceso, poniendo $A_1, A_2, \ldots, A_s$ debajo de $B_1, B_2, \ldots, B_s$. Esto dará una gráfica apropiada si y sólo si $s < t - 1$ o bien $s = t - 1$ y $B_t \neq A_s$.

En otras palabras, pueden moverse los $B_i$ si $t < s$ o bien si $t = s$ y $B_t \neq A_s$. Pueden moverse los $A_i$ si $s < t - 1$ o bien si $s = t - 1$ y $B_t \neq A_s$. No hay gráfica en la cual puedan moverse tanto los $A_i$ como los $B_i$. Las gráficas en las cuales no se tiene posibilidad son aquellas para las cuales $t = s$ y $B_t = A_s$ y aquellas para las cuales $s = t - 1$ y $B_t = A_s$. Partiendo de una partición $P$ para la cual pueden moverse los $A_i$, se obtiene una partición $P'$ que tiene los puntos $s$ que fueron movidos precisamente en el último renglón. Estos puntos están en la posición $B_i$ y, por supuesto, pueden regresarse a la partición $P$. Se llega a una situación semejante si la partición $P$ es tal que los $B_i$ pueden moverse. En ambos casos, el número de sumandos en $P'$ difiere en 1 del de $P$. Esto parea a todas las particiones de $n$ para las cuales pueden moverse los $A_i$ o bien los $B_i$, y en cualquier par $P, P'$, uno tiene un número par de sumandos, el otro tiene un número impar.

Consideremos las particiones excepcionales para las cuales no pueden moverse los $A_i$ ni los $B_i$, aquellas para las cuales $B_t = A_s$, $s = t$ o bien $t - 1$. Dado que $B_t = A_s$, la gráfica consiste de $s$ renglones. El renglón inferior tiene $t$ puntos y la partición es $n = a_1 + a_2 + \cdots + a_s$, $a_s = t$, $a_{s-1} = t + 1$, $a_1 = t + s - 1$. Por lo tanto, $n = st + (s - 1)s/2$. Si $s = t$, esto es $n = (3s^2 - s)/2$; y si $s = t - 1$, es $n = (3s^2 + s)/2$. Es fácil verificar que los enteros $(3s^2 \pm s)/2$, $s = 1, 2, \ldots$, todos son distintos. Por lo tanto se han pareado las particiones contadas por $q^e(n)$ con las contadas por $q^o(n)$, excepto para una sola partición en $s$ sumandos si $n = (3s^2 \pm s)/2$. Esto significa que

$$q^e(n) - q^o(n) = \begin{cases} (-1)^s & \text{Si } n = (3s^2 \pm s)/2 \text{ para algún } s = 1, 2, \cdots \\ 0 & \text{en cualquier otro caso.} \end{cases}$$

**Problema**

1. Denotemos por $p'(n)$ el número de particiones, $n = a_1 + a_2 + \cdots + a_r$, de $n$ en sumandos $a_1 \geqq a_2 \geqq a_3 \geqq \cdots \geqq a_r = 1$ tales que los $a_i$ consecutivos difieren cuando más en 1. Leer verticalmente las gráficas de tales particiones para probar que $p'(n) = p^d(n)$.

## 10.3 Funciones generadoras

Muchos resultados referentes a la función partición dependen de la teoría de las funciones analíticas y están más allá del alcance de este libro. No obstante, en las secciones siguientes se obtendrán algunos resultados interesantes sin la aplicación de mucho análisis. En esta sección se discuten heurísticamente las ideas principales sin considerar demostraciones cuidadosas. En realidad, nada se probará. El propósito de esta sección sólo es clarificar las ideas que se encuentran detrás de las demostraciones de las secciones posteriores.

La función $(1 - x^n)^{-1}$ tiene el desarrollo $\sum_{j=0}^{\infty} x^{jn}$. Tomando $n = 1, 2, \cdots, m$ y multiplicando se encuentra

$$\begin{aligned}\prod_{n=1}^{m} (1 - x^n)^{-1} &= (1 + x^{1\cdot 1} + x^{2\cdot 1} + \cdots)(1 + x^{1\cdot 2} + x^{2\cdot 2} + \cdots) \\ &\quad \times (1 + x^{1\cdot 3} + x^{2\cdot 3} + \cdots) \cdots \\ &\qquad (1 + x^{1\cdot m} + x^{2\cdot m} + \cdots) \\ &= \sum_{j_1=0}^{\infty} \sum_{j_2=0}^{\infty} \cdots \sum_{j_m=0}^{\infty} x^{j_1\cdot 1 + j_2\cdot 2 + \cdots + j_m\cdot m} \\ &= \sum_{j=0}^{\infty} c_j x^j\end{aligned}$$

donde $c_j$ es el número de soluciones de $j_1 \cdot 1 + j_2 \cdot 2 + \cdots + j_m \cdot m = n$ en los enteros no negativos $j_1, j_2, \cdots, j_m$. Esto es $c_j = p_m(j)$, y se tiene

$$\sum_{n=0}^{\infty} p_m(n) x^n = \prod_{n=1}^{m} (1 - x^n)^{-1}.$$

Este argumento, como lo demás en esta sección, es puramente formal.

Nada se dice acerca de la convergencia de la serie y no se ha puesto en duda lo referente a la multiplicación de series.

En forma semejante se encuentra

$$\sum_{n=0}^{\infty} p(n)x^n = \prod_{n=1}^{\infty} (1 - x^n)^{-1}.$$

La función $\prod_{n=1}^{\infty} (1 - x^n)^{-1}$ se llama la función generadora para $p(n)$, y la aplicación de los métodos analíticos a esta función conduce a los resultados respecto a $p(n)$.

La función generadora para $p_m(n)$ es $\prod_{n=1}^{m} ( - x^n)^{-1}$. De modo semejante, la función generadora para $p^o(n)$ se encuentra que es

$$\sum_{n=0}^{\infty} p^o(n)x^n = \prod_{n=1}^{\infty} (1 - x^{2n-1})^{-1},$$

y la función generadora para $p^d(n)$ es

$$\sum_{n=0}^{\infty} p^d(n)x^n = \prod_{n=1}^{\infty} (1 + x^n).$$

El Teorema 10.2 es equivalente a $\prod_{n=1}^{\infty} (1 + x^n) = \prod_{n=0}^{\infty} (1 - x^{2n-1})^{-1}$. Esta fórmula puede probarse directamente y después aplicarse para dar otra demostración del Teorema 10.2. Formalmente, por lo menos, se tiene

$$\begin{aligned}(1 - x^{2n-1})(1 + x^{2n-1})(1 + x^{2(2n-1)})(1 + x^{2^2(2n-1)}) \cdots \\ = (1 - x^{2(2n-1)})(1 + x^{2(2n-1)})(1 + x^{2^2(2n-1)}) \cdots \\ = (1 - x^{2^2(2n-1)})(1 + x^{2^2(2n-1)}) \cdots \\ = \cdots \\ = 1.\end{aligned}$$

Tomando $n = 1, 2, 3, \ldots$ y multiplicando se encuentra

$$\prod_{n=1}^{\infty} (1 - x^{2n-1}) \prod_{j=1}^{\infty} (1 + x^j) = 1$$

y

$$\prod_{j=1}^{\infty} (1 + x^j) = \prod_{n=1}^{\infty} (1 - x^{2n-1})^{-1}.$$

De modo semejante puede multiplicarse $\prod_{n=1}^{\infty} (1 - x^n)$ formalmente para obtener

$$\prod_{n=1}^{\infty} (1 - x^n) = \sum_{n=0}^{\infty} (q^e(n) - q^o(n))x^n$$

Entonces el Teorema 10.4 implica

$$\prod_{n=1}^{\infty} (1 - x^n) = 1 + \sum_{j=1}^{\infty} (-1)^j(x^{(3j^2+j)/2} + x^{(3j^2-j)/2}).$$

Esto se conoce como fórmula de Euler. Se demuestra en el Teorema 10.8.

**Problema**

1. Demostrar que el producto infinito

$$(1 + x_1)(1 + x_1x_2)(1 + x_1x_2x_3) \cdots = 1 + \sum x_1^{a_1}x_2^{a_2} \cdots x_k^{a_k}$$

donde $a_i - a_{i+1}$ es 0 o bien 1 y $a_k = 1$. Contar el número de términos en el desarrollo que sean de grado $n$. Hacer $x_1 = x_2 = x_3 = \cdots = x$ para demostrar que $(1 + x)(1 + x^2)(1 + x^3) \cdots$ es la función generadora para $p'(n)$ del Problema 1, Sección 10.2.

## 10.4 Fórmula de Euler

En esta sección se probarán algunas de las cosas desarrolladas en la Sección 10.3. Al hacerlo sólo se aplicarán hechos rudimentarios referentes a las series infinitas y a los límites. Un lector familiarizado con la teoría de las funciones analíticas reconocerá que nuestras funciones son analíticas en $|x| < 1$ y será capaz de acortar sus demostraciones.

**Teorema 10.5** *Supóngase que* $0 \leqq x < 1$ *y sea* $\varphi_m(x) = \prod_{n=1}^{m} (1 - x^n)$. *Entonces* $\sum_{n=0}^{\infty} p_m(n) x^n$ *converge y*

$$\sum_{n=0}^{\infty} p_m(n)x^n = \frac{1}{\varphi_m(x)}.$$

*Demostración.* Por el Teorema 10.3, $p_m(n)$ es igual al número de particiones de $n$ en cuando más $m$ sumandos. Este es el mismo que el número de particiones en exactamente $m$ sumandos si se admiten sumandos cero. Entonces cada sumando es 0 o bien 1 o bien 2 o bien . . . o bien $n$ y se tiene $p_m(n) \leqq (n + 1)^m$. La serie $\sum_{n=0}^{\infty} (n + 1)^m x^n$ converge, por la prueba de la razón, y de aquí que, por la prueba de comparación, $\sum_{n=0}^{\infty} p_m(n) x^n$ también converge.

Ahora bien

$$(1 - x^{m!k})^m \varphi_m(x)^{-1} = \prod_{n=1}^{m} \frac{1 - x^{m!k}}{1 - x^n} = \prod_{n=1}^{m} \frac{1 - (x^n)^{(m!/n)k}}{1 - x^n}$$

$$= \prod_{n=1}^{m} \sum_{j=0}^{(m!/n)k-1} x^{jn} = \sum_h c_h x^h$$

donde la última suma es una suma finita y $0 \leqq c_h \leqq p_m(h)$ para todo $h = 0, 1, 2, \cdots$, y $c_h = p_m(h)$ si $h < m!k$. Por tanto se tiene

$$\sum_{h=0}^{m!k-1} p_m(h)x^h \leqq (1 - x^{m!k})^m \varphi_m(x)^{-1} \leqq \sum_{h=0}^{\infty} p_m(h)x^h.$$

Conforme $k \to \infty$ se tiene

$$\sum_{h=0}^{m!k-1} p_m(h)x^h \to \sum_{h=0}^{\infty} p_m(h)x^h, \qquad (1 - x^{m!k})^m \to 1,$$

y de aquí que

$$\varphi_m(x)^{-1} = \sum_{h=0}^{\infty} p_m(h)x^h.$$

**Teorema 10.6** *Para* $0 \leqq x < 1$, $\lim_{m\to\infty} \varphi_m(x)$ *existe y es diferente de cero. Hagamos* $\varphi(x) = \lim_{m\to\infty} \varphi_m(x)$ *y definamos* $\prod_{n=1}^{\infty} (1 - x^n)$ *como* $\varphi(x)$.

*Demostración.* Dado que $\varphi_m(0) = 1$ el resultado es obvio para $x = 0$. Para $x > 0$ se aplica el teorema del valor medio a la función $\log z$ para obtener un $y$ tal que $1 - x^n < y < 1$ y

$$\frac{\log 1 - \log(1 - x^n)}{1 - (1 - x^n)} = \frac{1}{y}.$$

Por lo tanto

$$-\log(1 - x^n) = \frac{x^n}{y}, \qquad -\log(1 - x^n) \leqq \frac{x^n}{1 - x^n} \leqq \frac{x^n}{1 - x}$$

y de aquí que

$$-\log \varphi_m(x) = \sum_{n=1}^{m} -\log(1 - x^n) \leqq \sum_{n=1}^{m} \frac{x^n}{1 - x} \leqq \frac{1 - x^{m+1}}{(1 - x)^2} < \frac{1}{(1 - x)^2}.$$

Esto demuestra que $-\log \varphi_m(x)$, y por tanto $\varphi_m(x)^{-1}$, es acotada para un $x$ fijo conforme $m \to \infty$.

Pero

$$\varphi_m(x)^{-1} = \prod_{n=1}^{m} \frac{1}{1 - x^n}$$

se incrementa monótonamente para $x$ fijo cuando $m \to \infty$. Dado que $\varphi_1(x)^{-1} = 1/(1 - x) > 0$ esto demuestra que $\lim_{m\to\infty} \varphi_m(x)^{-1}$ existe y es diferente de cero. Por lo tanto $\lim_{m\to\infty} \varphi_m(x)$ existe y también es diferente de cero.

**Teorema 10.7** *Para* $0 \leqq x < 1$, *la serie* $\sum_{n=0}^{\infty} p(n)x^n$ *converge y* $\sum_{n=0}^{\infty} p(n)x^n = \varphi(x)^{-1}$.

*Demostración.* Se tiene, aplicando el Teorema 10.5,

$$\sum_{n=0}^{m} p(n)x^n = \sum_{n=0}^{m} p_m(n)x^n \leqq \sum_{n=0}^{\infty} p_m(n)x^n = \varphi_m(x)^{-1} \leqq \varphi(x)^{-1}.$$

Para $x$ fijo, $\sum_{n=0}^{m} p(n)x^n$ se incrementa conforme $m \to \infty$. Por lo tanto $\sum_{n=0}^{\infty} p(n)x^n = \lim_{m\to\infty} \sum_{n=0}^{\infty} p(n)x^n$ existe y es $\leqq \varphi(x)^{-1}$.

Pero ahora

$$\sum_{n=0}^{\infty} p(n)x^n \geqq \sum_{n=0}^{\infty} p_m(n)x^n = \varphi_m(x)^{-1}.$$

Haciendo $m \to \infty$ se tiene $\sum_{n=0}^{\infty} p(n)x^n \geqq \varphi(x)^{-1}$ y de aquí que $\sum_{n=0}^{\infty} p(n)x^n = \varphi(x)^{-1}$.

**Teorema 10.8** *Fórmula de Euler. Para* $0 \leqq x < 1$ *se tiene*

$$\varphi(x) = 1 + \sum_{j=1}^{\infty} (-1)^j (x^{(3j^2+j)/2} + x^{(3j^2-j)/2}).$$

*Demostración.* La prueba de la razón demuestra que $\sum_{j=1}^{\infty} x^{(3j^2\pm j)/2}$ converge; por tanto, también converge la serie anterior. Sea $q_m^e(n)$ el número de particiones de $n$ en un número par de sumandos distintos no mayor que $m$, y sea $q_m^o(n)$ el número de particiones de $n$ en un número impar de sumandos distintos no mayores que $m$ Como en la definición 10.2, se tomará $q_m^e(0) = 1$, $q_m^o(0) = 0$. Entonces

(10.1) $$\varphi_m(x) = (1 - x)(1 - x^2)(1 - x^3) \cdots (1 - x^m) = \sum_n (q_m^e(n) - q_m^o(n))x^n,$$

una suma finita. Pero para $n \leqq m$ se tiene $q_m^e(n) = q^e(n)$, $q_m^o(n) = q^o(n)$ y también se tienen $q_m^e(n) + q_m^o(n) \leqq p(n)$ para todo $n$.

Por tanto

$$\left| \varphi_m(x) - \sum_{n=0}^{m} (q^e(n) - q^o(n))x^n \right|$$

$$\leqq \sum_{n>m} |q_m^e(n) - q_m^o(n)|x^n \leqq \sum_{n=m+1}^{\infty} p(n)x^n.$$

Dado que $\sum_{n=m+1}^{\infty} p(n)x^n \to 0$ conforme $m \to \infty$, se obtiene $\sum_{n=0}^{\infty} (q^e(n) - q^o(n))\, x^n = \varphi(x)$ haciendo $m \to \infty$. Aplicando el Teorema 10.4, se tiene el presente teorema.

Tendremos ocasión de multiplicar series de potencias. Por ello necesitamos el siguiente lema.

**Lema 10.9** *Sean* $\sum_{j=0}^{\infty} a_j x^j$ y $\sum_{k=0}^{\infty} b_k x^k$ *absolutamente convergentes para* $0 \leqq x < 1$. *Entonces* $\sum_{h=0}^{\infty} \left( \sum_{j=0}^{h} a_j b_{h-j} \right) x^h$ *converge y tiene el valor* $\sum_{j=0}^{\infty} a_j x_j \sum_{k=0}^{\infty} b_k x^k$ *para* $0 \leqq x < 1$.

*Demostración.* La condición $0 \leqq x < 1$ podría reemplazarse por $|x| < 1$; tenemos $0 \leqq x < 1$ precisamente para mantener el lema en concordancia con los demás teoremas. Las sumas $\sum_{j=0}^{m} a_j x^j$ y $\sum_{k=0}^{m} b_k x^k$ son polinomios y pueden multiplicarse mediante las reglas usuales del álgebra. Los términos de grado $m$ o menor en el producto de los polinomios son precisamente los términos en

$$\sum_{h=0}^{m} \left( \sum_{j=0}^{h} a_j b_{h-j} \right) x^h.$$

Todos los demás términos en el producto son de la forma $a_j b_k x^{j+k}$ con $j + k > m$. Puesto que $j + k > m$ implica que por lo menos uno de $j$ y $k$ excede a $[m/2]$, se ve que

$$\sum_{j=0}^{m} a_j x^j \sum_{k=[m/2]}^{m} b_k x^k + \sum_{j=[m/2]}^{m} a_j x^j \sum_{k=0}^{m} b_k x^k,$$

cuando se multiplica será una suma de términos que incluye todos los términos $a_j b_k x^{j+k}$, $j + k > m$ y posiblemente otros. Esto implica que

$$\left|\sum_{j=0}^{m} a_j x^j \sum_{k=0}^{m} b_k x^k - \sum_{h=0}^{m}\left(\sum_{j=0}^{m} a_j b_{h-j}\right)x^h\right|$$

$$\leqq \sum_{j=0}^{m} |a_j x^j| \sum_{k=[m/2]}^{m} |b_k x^k| + \sum_{j=[m/2]}^{m} |a_j x^j| \sum_{k=0}^{m} |b_k x^k|$$

$$\leqq \sum_{j=0}^{\infty} |a_j x^j| \sum_{k=[m/2]}^{\infty} |b_k x^k| + \sum_{j=[m/2]}^{\infty} |a_j x^j| \sum_{k=0}^{\infty} |b_k x^k|,$$

dado que las cuatro series infinitas en esta última expresión son convergentes. Haciendo $m \to \infty$ se ve que $\sum_{h=0}^{\infty}\left(\sum_{j=0}^{h} a_j b_{h-j}\right)x^h$ converge y es igual a $\sum_{n=0}^{\infty} a_j x^j \sum_{k=0}^{\infty} b_k x^k$.

Este lema implica que si $\sum_{j=0}^{\infty} a_j x^j$ y $\sum_{k=0}^{\infty} b_k x^k$ convergen absolutamente para $0 \leqq x < 1$, entonces $\sum_{h=0}^{\infty}\left(\sum_{j=0}^{h} a_j b_{h-j}\right)x^h$. Aplicándolo a $\sum_{j=0}^{\infty} |a_j| x^j$ y $\sum_{k=0}^{\infty} |b_k| x^k$, se encuentra que $\sum_{j=0}^{\infty}\left(\sum_{j=0}^{h} |a_j b_{h-j}|\right)x^h$ converge para $0 \leqq x < 1$. Puesto que $\left|\sum_{j=0}^{h} a_j b_{h-j}\right| \leqq \sum_{j=0}^{h} |a_j b_{h-j}|$, se ve que $\sum_{h=0}^{\infty}\left(\sum_{j=0}^{h} a_j b_{h-j}\right) x^h$ converge absolutamente para $0 \leqq x < 1$. Entonces el lema puede extenderse al producto de cualquier número finito de series de potenciales $\sum_{j=0}^{\infty} a_j^{(i)} x^j$ que sean convergentes absolutamente para $0 \leqq x < 1$.

Otro hecho que se usará es el siguiente:

**Lema 10.10** *Si* $\sum_{j=0}^{\infty} a_j x^j$ *y* $\sum_{j=0}^{\infty} b_j x^j$ *convergen absolutamente y* $\sum_{j=0}^{\infty} a_j x^j = \sum_{j=0}^{\infty} b_j x^j$ *para* $0 \leqq x < 1$, *entonces* $a_j = b_j$ *para todo* $j = 0, 1, 2, \ldots$.

*Demostración.* Si $c_j = a_j - b_j$, entonces $|c_j x^j| \leqq |a_j x^j| + |b_j x^j|$ y de aquí que $\sum_{j=0}^{\infty} c_j x^j$ converge absolutamente para $0 \leqq x < 1$ y sólo se necesita demostrar que $\sum_{j=0}^{\infty} c_j x^j = 0$ implica $c_j = 0$. Haciendo $x = 0$ tenemos $c_0 =$ . Supóngase que el lema es falso. Entonces existe algún $c_j \neq 0$, y puede hacerse $k$ el menor entero positivo para el cual $c_k \neq 0$. Entonces $\sum_{j=0}^{\infty} c_j x^j = \sum_{j=k}^{\infty} c_j x^j$ y, debido a que esta serie converge absolutamente para $x = \frac{1}{2}$, existe un entero $m > k$ tal que $\sum_{j=m+1}^{\infty} |c_j 2^{-j}| < 2^{-k-1}|c_k|$. Ahora, para $0 < x < 1$ se tiene $\sum_{j=k}^{\infty} c_j x^j = 0$ y, dividiendo entre $x^k$, se obtiene

$$c_k + \sum_{j=k+1}^{m} c_j x^{j-k} + \sum_{j=m+1}^{\infty} c_j x^{j-k} = 0.$$

Entonces, para $0 < x \leqq \frac{1}{2}$, puede escribirse

$$\begin{aligned} |c_k| &\leqq \left| \sum_{j=k+1}^{m} c_j x^{j-k} \right| + \left| \sum_{j=m+1}^{\infty} c_j x^{j-k} \right| \\ &\leqq \left| \sum_{j=k+1}^{m} c_j x^{j-k} \right| + \sum_{j=m+1}^{\infty} |c_j| x^{j-k} \\ &\leqq \left| \sum_{j=k+1}^{m} c_j x^{j-k} \right| + \sum_{j=m+1}^{\infty} |c_j| 2^{-j+k} \\ &< |c_{k+1}x + c_{k+2}x^2 + \cdots + c_m x^{m-k}| + 2^k \cdot 2^{-k-1}|c_k|, \end{aligned}$$

y finalmente

$$\tfrac{1}{2}|c_k| < |c_{k+1}x + c_{k+2}x^2 + \cdots + c_m x^{m-k}|.$$

Pero $c_{k+1}x + c_{k+2}x^2 + \cdots + c_m x^{m-k}$ es un polinomio y su valor puede hacerse menor que el número positivo $|c_k|/2$; escogiendo $x$ lo suficientemente próximo a cero, $0 < x \leqq \frac{1}{2}$. Esto es una contradicción, y por tanto, el lema queda demostrado.

Ahora podemos regresar a la función partición.

**Teorema 10.11** *Si* $n \geqq 1$ *entonces*

$$\begin{aligned} p(n) &= p(n-1) + p(n-2) - p(n-5) - p(n-7) \\ &+ p(n-12) + p(n-15) - \cdots = \sum_{j} (-1)^{j+1} p(n - \tfrac{1}{2}(3j^2 \pm j)) \end{aligned}$$

*donde la suma se extiende sobre todos los enteros positivos para los cuales los argumentos de la función partición son no negativos.*

*Demostración.* Con base en los Teoremas 10.7 y 10.8 se tiene

$$\left(1 + \sum_{j=1}^{\infty} (-1)^j (x^{(3j^2+j)/2} + x^{(3j^2-j)/2})\right) \sum_{k=0}^{\infty} p(k) x^k = \varphi(x)\varphi(x)^{-1} = 1$$

si $0 \leqq x < 1$; esto es

$$(1 - x - x^2 + x^5 + x^7 - x^{12} - x^{15} + \cdots) \sum_{k=0}^{\infty} p(k)x^k = 1.$$

Aplicando el Lema 10.9 se encuentra

$$\sum_{h=0}^{\infty} (p(h) - p(h-1) - p(h-2) + p(h-5) + p(h-7) - \cdots)x^h = 1,$$

lo cual, por el Lema 10.10, implica $p(h) - p(h-1) - p(h-2) + \cdots = 0$.

El teorema que se acaba de probar puede usarse para construir una tabla de $p(n)$. Existe una fórmula semejante para la función $\sigma(n)$, la suma de los divisores de $n$.

**Teorema 10.12** *Para $n \geqq 1$ se tiene*

$$\sigma(n) - \sigma(n-1) - \sigma(n-2) + \sigma(n-5) + \sigma(n-7) - \sigma(n-12) - \sigma(n-15) + \cdots = \begin{cases} (-1)^{j+1}n \text{ si } n = \dfrac{3j^2 \pm j}{2} \\ 0 \textit{ en cualquier otro caso} \end{cases}$$

*donde la suma se extiende mientras los argumentos son positivos.*

*Demostración.* Tomando la derivada de $\varphi_m(x) = \log \prod_{n=1}^{m} (1 - x^n)$ se obtiene

$$\frac{\varphi_m'(x)}{\varphi_m(x)} = \sum_{n=1}^{m} \frac{-nx^{n-1}}{1 - x^n} = \sum_{n=1}^{m} \sum_{j=1}^{\infty} -nx^{jn-1} = \sum_{n=1}^{m} \sum_{k=1}^{\infty} c_{n,k}x^{k-1}$$

para $0 \leqq x < 1$, donde

$$c_{n,k} = \begin{cases} -n \text{ si } n|k \\ 0 \text{ en cualquier otro caso} \end{cases}$$

Hay $m$ series $\sum_{k=1}^{\infty} c_{n,k}x^{k-1}$, cada una de las cuales converge absolutamente. Pueden sumarse término a término para dar

$$\frac{\varphi_m'(x)}{\varphi_m(x)} = \sum_{k=1}^{\infty} \left( \sum_{n=1}^{m} c_{n,k} \right) x^{k-1} \tag{10.2}$$

Aplicando, (10.1) se tiene $\varphi_m'(x) = \sum_n n(q_m^e(n) - q_m^o(n))x^{n-1}$ puesto que $\varphi_m(x)$ es una suma finita, un polinomio en $x$. Pero también puede escribirse (10.1) en la forma de una serie infinita

$$\varphi_m(x) = \sum_{n=0}^{\infty} (q_m^e(n) - q_m^o(n))x^n$$

en la cual todos los términos desde un cierto $n$ en adelante son cero. Entonces la ecuación (10.2) puede ponerse en la forma

$$\sum_n n(q_m^e(n) - q_m^o(n))x^{n-1} = \sum_{n=0}^{\infty} (q_m^e(n) - q_m^o(n))x^n \sum_{j=0}^{\infty}\left(\sum_{i=1}^{m} c_{i,j+1}\right)x^j$$
$$= \sum_{h=0}^{\infty}\left(\sum_{n=0}^{h} (q_m^e(n) - q_m^o(n)) \sum_{i=1}^{m} c_{i,h-n+1}\right)x^h$$

por el Lema 10.9. Entonces el Lema 10.10 nos da

$$k(q_m^e(k) - q_m^o(k)) = \sum_{n=0}^{k-1} (q_m^e(n) - q_m^o(n)) \sum_{i=1}^{m} c_{i,k-n}.$$

Para cualquier $k$ dado puede escogerse $m > k$. Entonces $q_m^e(k) = q^e(k)$, $q_m^o(k) = q^o(k)$, $q_m^e(n) = q^e(n)$, $q_m^o(n) = q^o(n)$ y $\sum_{i=1}^{m} c_{i,k-n} = -\sum_{d|k-n} d = -\sigma(k-n)$ para $n \leqq k-1$. Esto con el Teorema 10.4 nos da

$$-\sigma(k) + \sigma(k-1) + \sigma(k-2) - \sigma(k-5) - \sigma(k-7) + \cdots = \begin{cases} (-1)^j k \text{ si } k = \dfrac{3j^2 \pm j}{2} \\ 0 \text{ en cualquier otro caso} \end{cases}$$

y el teorema queda demostrado.

**Problemas**

1. Calcular una tabla corta de los valores de $p(n)$, de $n = 1$ hasta $n = 20$, mediante la aplicación del Teorema 10.11.
2. Calcular una tabla corta de los valores de $\sigma(n)$, de $n = 1$ hasta $n = 20$, por medio del Teorema 10.12. Verificar las anotaciones, calculando directamente $\sigma(n) = \sum_{d|n} d$.

## 10.5 Fórmula de Jacobi

**Teorema 10.13** *Fórmula de Jacobi. Para* $0 \leqq x < 1$,

$$\varphi(x)^3 = \sum_{j=0}^{\infty} (-1)^j(2j+1)x^{(j^2+j)/2}.$$

*Demostración.* La fórmula es obvia para $x = 0$, de modo que puede suponerse $0 < x < 1$. Para $0 < q < 1$, $0 < z < 1$, se define

$$(10.3)\quad f_n(z) = \prod_{k=1}^{n} \{(1 - q^{2k-1}z^2)(1 - q^{2k-1}z^{-2})\} = \sum_{j=-n}^{n} a_j z^{2j}$$

donde los $a_j$ son polinomios en $q$. Dado que $f_n(1/z) = f_n(z)$ se tiene $a_{-j} = a_j$, y es fácil ver que

$$(10.4)\qquad a_n = (-1)^n q^{1+3+5+\cdots+(2n-1)} = (-1)^n q^{n2}.$$

Para obtener las otros $a_j$ se reemplaza $z$ por $qz$ en (10.3) y se encuentra

$$f_n(qz) = \prod_{k=1}^{n} \{(1 - q^{2k+1}z^2)(1 - q^{2k-3}z^{-2})\}$$

$$= \prod_{k=2}^{n+1} (1 - q^{2k-1}z^2) \prod_{j=0}^{n-1} (1 - q^{2j-1}z^{-2})$$

y de aquí que

$$qz^2(1 - q^{2n-1}z^{-2})f_n(qz)$$

$$= (1 - q^{2n+1}z^2) \left\{\prod_{k=2}^{n} (1 - q^{2k-1}z^2)\right\} qz^2(1 - q^{-1}z^{-2}) \prod_{j=1}^{n} (1 - q^{2j-1}z^{-2})$$

$$= -(1 - q^{2n+1}z^2) \prod_{k=1}^{n} (1 - q^{2k-1}z^2) \prod_{j=1}^{n} (1 - q^{2j-1}z^{-2})$$

$$= (q^{2n+1}z^2 - 1)f_n(z).$$

Si se escriben las funciones $f_n$ en términos de los $a_j$, aplicando (10.3), e igualando los coeficientes de $z^{2k}$, se encuentra

$$qa_{k-1}q^{2k-2} - q^{2n}a_k q^{2k} = q^{2n+1}a_{k-1} - a_k$$

y entonces

$$a_{k-1} = \frac{-(1 - q^{2n+2k})}{q^{2k-1}(1 - q^{2n-2k+2})}\, a_k.$$

Esto, junto con (10.4) nos permite, a su vez, encontrar $a_{n-1}, a_{n-2}, \ldots .$ De hecho para $0 < j \leqq n$ se encuentra

$$a_{n-j} = \frac{(-1)^j(1 - q^{4n})(1 - q^{4n-2}) \cdots (1 - q^{4n-2j+2})}{(1 - q^2)(1 - q^4) \cdots (1 - q^{2j})} (-1)^n q^{(n-j)2}$$

y de aquí que

$$(10.5) \quad a_k = \frac{\prod_{h=n+k+1}^{2n} (1 - q^{2h})}{\prod_{h=1}^{n-k} (1 - q^{2h})} (-1)^k q^{k^2} = \frac{\varphi_{2n}(q^2)}{\varphi_{n+k}(q^2)\varphi_{n-k}(q^2)} (-1)^k q^{k^2}.$$

Esta fórmula esa válida para $0 \leqq k \leqq n$ si se conviene en tomar $\varphi_0(q^2) = 1$.

Regresando a (10.3), se ve que $f_n(z)$ es un producto de $2n$ factores, uno de los cuales es $(1 - qz^{-2})$, el cual tiene el valor 0 en $z = q^{1/2}$. Por tanto, tomando la derivada y a continuación haciendo $z = q^{1/2}$ se tiene

$$f_n'(q^{1/2}) = \prod_{k=1}^{n} (1 - q^{2k-1}q) \left\{ \prod_{j=2}^{n} (1 - q^{2j-1}q^{-1}) \right\} 2qq^{-3/2}$$

$$= \frac{2q^{-1/2}}{1 - q^{2n}} \varphi_n(q^2)^2.$$

Por otra parte, de (10.3), también se tiene

$$f_n'(q^{1/2}) = \sum_{j=-n}^{n} 2ja_j q^{j-1/2} = \sum_{j=1}^{n} 2ja_j q^{-1/2}(q^j - q^{-j}).$$

Así que se encuentra

$$\varphi_n(q^2)^2 = (1 - q^{2n}) \sum_{j=1}^{n} ja_j(q^j - q^{-j}),$$

y de aquí que, por (10.5),

$$\varphi_n(q^2)^3 = (1 - q^{2n}) \sum_{j=1}^{n} (-1)^j j q^{j^2}(q^j - q^{-j}) \frac{\varphi_{2n}(q^2)\varphi_n(q^2)}{\varphi_{n+j}(q^2)\varphi_{n-j}(q^2)}.$$

Ahora bien

$$0 \leqq \frac{\varphi_{2n}(q^2)\varphi_n(q^2)}{\varphi_{n+j}(q^2)\varphi_{n-j}(q^2)} = \prod_{h=n+j+1}^{2n} (1 - q^{2h}) \prod_{k=n-j+1}^{n} (1 - q^{2k}) \leqq 1,$$

y $\sum_{k=1}^{\infty} jq^{j^2}|q^j - q^{-j}|$ converge, de donde, para $n > m$, se tiene

$$\left| \varphi_n(q^2)^3 - (1 - q^{2n}) \sum_{j=1}^{m} (-1)^j j q^{j^2}(q^j - q^{-j}) \frac{\varphi_{2n}(q^2)\varphi_n(q^2)}{\varphi_{n+j}(q^2)\varphi_{n-j}(q^2)} \right|$$

$$\leqq \sum_{j=m+1}^{n} jq^{j^2}|q^j - q^{-j}| \leqq \sum_{j=m+1}^{\infty} jq^{j^2}|q^j - q^{-j}|.$$

Se mantiene $k$ fijo pero arbitrario y hacemos $n \to \infty$. Por el Teorema 10.6 se tiene

$$\lim_{n\to\infty} \frac{\varphi_{2n}(q^2)\,\varphi_n(q^2)}{\varphi_{n+j}(q^2)\,\varphi_{n-j}(q^2)} = \frac{\varphi(q^2)^2}{\varphi(q^2)^2} = 1$$

y $\lim_{n\to\infty} \varphi_n(q^2)^3 = \varphi(q^2)^3$ de modo que se obtiene

$$\left|\varphi(q^2)^3 - \sum_{j=1}^{m} (-1)^j j q^{j^2}(q^j - q^{-j})\right| \leqq \sum_{j=m+1}^{\infty} j q^{j^2}|q^j - q^{-j}|.$$

Ahora, haciendo $m \to \infty$ se encuentra

$$\varphi(q^2)^3 = \sum_{j=1}^{\infty} (-1)^j j q^{j^2}(q^j - q^{-j}) = \sum_{j=1}^{\infty} (-1)^j j q^{j^2+j} + \sum_{j=1}^{\infty} (-1)^{j-1} j q^{j^2-j}$$

donde puede efectuarse el último paso debido a que ambas series convergen. Cambiando $j$ a $j+1$, se escribe la última serie como $\sum_{j=0}^{\infty} (-1)^j (j+1)q^{j^2+j}$ y entonces puede sumarse a la primera serie para obtener

$$\varphi(q^2)^3 = \sum_{j=0}^{\infty} (-1)^j (2j+1) q^{j^2+j}.$$

Esto es el teorema con $x$ reemplazada por $q^2$.

**Problema**

1. Reemplazar $z$ por $q^{1/6}$ en (10.3), multiplicar por $\varphi_n(q^2)$ y aplicar (10.5) para obtener una demostración de la fórmula de Euler

## 10.6 Una propiedad de divisibilidad

**Teorema 10.14** *Si $p$ es un primo y $0 \leqq x < 1$ entonces*

$$\frac{\varphi(x^p)}{\varphi(x)^p} = 1 + p \sum_{j=1}^{\infty} a_j x^j$$

*donde los $a_j$ son enteros.*

*Demostración.* Para $0 \leqq u < 1$ se tiene el desarrollo

$$(1-u)^{-p} = 1 + \sum_{j=1}^{\infty} (-1)^j \frac{(-p)(-p-1)\cdots(-p-j+1)}{j!} u^j$$

$$= 1 + \sum_{j=1}^{\infty} \frac{(p+j-1)!}{j!(p-1)!} u^j = \sum_{j=0}^{\infty} b_j u^j,$$

y por tanto, digamos,

$$\frac{1-u^p}{(1-u)^p} = (1-u)^{-p} - u^p(1-u)^{-p} = \sum_{j=0}^{\infty} b_j u^j - \sum_{j=0}^{\infty} b_j u^{j+p}$$

$$= \sum_{j=0}^{p-1} b_j u^j + \sum_{j=p}^{\infty} (b_j - b_{j-p})u^j = \sum_{j=0}^{\infty} c_j u^j,$$

Pero

$$b_j = \frac{(j+1)(j+2)\cdots(j+p-1)}{(p-1)!}$$

$$\equiv \begin{cases} 1 \pmod p & \text{si } j \equiv 0 \pmod p \\ 0 \pmod p & \text{si } j \not\equiv 0 \pmod p, \end{cases}$$

y $b_0 < b_1 < b_2 < \cdots$, de modo que se tiene $c_0 = b_0 = 1$, $c_j > 0$, $c_j \equiv 0 \pmod p$ para $j > 0$.

Ahora, para $0 \leqq x < 1$,

$$\frac{\varphi_m(x^p)}{\varphi_m(x)^p} = \prod_{n=1}^{m} \frac{1-x^{pn}}{(1-x^n)^p} = \sum_{j=0}^{\infty} a_j^{(m)} x^j$$

donde $a_j^{(1)} = c_j$ y, por el Lema 10.9,

$$\sum_{h=0}^{\infty} a_h^{(m)} x^h = \sum_{j=0}^{\infty} c_j x^{mj} \sum_{k=0}^{\infty} a_k^{(m-1)} x^k = \sum_{h=0}^{\infty} \sum_{j=0}^{[h/m]} c_j a_{h-mj}^{(m-1)} x^h.$$

Entonces, por el Lema 10.10, se tiene

$$a_h^{(m)} = \sum_{j=0}^{[h/m]} c_j a_{h-mj}^{(m-1)},$$

y de aquí que

$$a_h^{(m)} \equiv a_h^{(m-1)} \equiv a_h^{(1)} \equiv c_h \pmod p,$$
$$a_h^{(m)} \geqq a_h^{(m-1)} \geqq a_h^{(1)} = c_h > 0,$$
$$a_h^{(m)} = a_h^{(m-1)} \text{ si } h \leqq m-1.$$

Por tanto

$$\sum_{h=0}^{m} a_h^{(h)} x^h = \sum_{h=0}^{m} a_h^{(m)} x^h \leqq \sum_{h=0}^{\infty} a_h^{(m)} x^h = \frac{\varphi_m(x^p)}{\varphi_m(x)^p}.$$

Dado que la suma de la izquierda se incrementa conforme $m \to \infty$ se ve que $\sum_{h=0}^{\infty} a_h^{(h)} x^h$ converge y

$$\sum_{h=0}^{\infty} a_h^{(h)} x^h \leqq \frac{\varphi(x^p)}{\varphi(x)^p}.$$

Pero también se tiene

$$\sum_{h=0}^{\infty} a_h^{(h)} x^h = \sum_{h=0}^{m} a_h^{(m)} x^h + \sum_{h=m+1}^{\infty} a_h^{(h)} x^h$$

$$\geqq \sum_{h=0}^{m} a_h^{(m)} x^h + \sum_{h=m+1}^{\infty} a_h^{(m)} x^h = \frac{\varphi_m(x^p)}{\varphi_m(x)^p},$$

$$\sum_{h=0}^{\infty} a_h^{(h)} x^h \geqq \frac{\varphi(x^p)}{\varphi(x)^p},$$

y finalmente

$$\sum_{h=0}^{\infty} a_h^{(h)} x^h = \frac{\varphi(x^p)}{\varphi(x)^p}.$$

Dado que $a_0^{(0)} = c_0 = 1$ y $a_h^{(h)} \equiv c_h \equiv 0 \pmod{p}$ para $h \geqq 1$, el teorema queda demostrado.

**Teorema 10.15** *Para* $0 \leqq x < 1$ *se tiene* $x\varphi(x)^4 = \sum_{m-1}^{\infty} b_m x^m$ *donde los* $b_m$ *son enteros y* $b_m \equiv 0 \pmod{5}$ *si* $m \equiv 0 \pmod{5}$.

*Demostración.* Puede escribirse el Teorema 10.8 en la forma

$$\varphi(x) = \sum_{k=0}^{\infty} c_k x^k, \qquad c^k = \begin{cases} (-1)^j & \text{si } k = (3j^2 \pm j)/2 \\ 0 & \text{en cualquier otro caso} \end{cases}$$

y el Teorema 10.13 como

$$\varphi(x)^3 = \sum_{n=0}^{\infty} d_n x^n, \qquad d_n = \begin{cases} (-1)^j(2j+1) & \text{si } n = (j^2 + j)/2 \\ 0 & \text{en cualquier otro caso} \end{cases}$$

y entonces se aplica el Lema 10.9 para obtener

$$x\varphi(x)^4 = x\varphi(x)\varphi(x)^3$$

$$= x \sum_{h=0}^{\infty} \left( \sum_{k=0}^{h} c_k d_{h-k} \right) x^h = \sum_{m=1}^{\infty} b_m x^m.$$

Entonces $b_m = \sum_{k=0}^{m-1} c_k d_{m-1-k}$ puede escribirse como $\sum c_k d_n$ sumado sobre todo $k \geqq 0$, $n \geqq 0$, tales que $k + n = m - 1$. Pero $d_n$ es 0 a menos que $n = (j^2 + j)/2$, $j = 0, 1, 2, \ldots$, en cuyo caso es $(-1)^j(2j + 1)$. Además puede describirse $c_k$ diciendo que es 0 a menos que $k = (3i^2 +$

$i)/2$, $i = 0, \pm 1, \pm 2, \ldots$, en cuyo caso es $(-1)^i$. Entonces puede escribirse

$$(10.6) \quad b_m = \sum (-1)^i(-1)^j(2j+1) = \sum (-1)^{i+j}(2j+1)$$

sumado sobre todo $i$ y $j$ tales que $j \geqq 0$ y $(3i^2+i)/2 + (j^2+j)/2 = m-1$. Pero

$$2(i+1)^2 + (2j+1)^2 = 8\left(1 + \frac{3i^2+i}{2} + \frac{j^2+j}{2}\right) - 10i^2 - 5$$

de modo que si $m \equiv 0 \pmod 5$, los términos en (10.6) tendrán que ser tales que $2(i+1)^2 + (2j+1)^2 \equiv 0 \pmod 5$. Es decir $(2j+1)^2 \equiv -2(i+1)^2 \pmod 5$. Sin embargo, $-2$ es un no residuo cuadrático módulo 5, de manera que esta condición implica $2j+1 \equiv 0 \pmod 5$ y de aquí que $b_m \equiv 0 \pmod 5$ si $m \equiv 0 \pmod 5$.

**Teorema 10.16** *Se tiene* $p(5m+4) \equiv 0 \pmod 5$.

*Demostración.* Por los Teoremas 10.15, 10.14 y 10.7 se tiene

$$\sum_{n=0}^{\infty} p(n)x^{n+1} = \frac{x}{\varphi(x)} = x\varphi(x)^4 \frac{\varphi(x^5)}{\varphi(x)^5} \frac{1}{\varphi(x^5)}$$

$$= \sum_{m=1}^{\infty} b_m x^m \left(1 + 5\sum_{j=1}^{\infty} a_j x^j\right) \sum_{k=0}^{\infty} p(k)x^{5k}$$

donde los $a_j$ y los $b_m$ son enteros y $b_m \equiv 0 \pmod 5$ para $m \equiv 0 \pmod 5$. Aplicando los Lemas 10.9 y 10.10 se encuentra que

$$p(n-1) \equiv \sum_{k=0}^{[n/5]} p(k) b_{n-5k} \pmod 5$$

y de aquí que $p(5m+4) \equiv 0 \pmod 5$ dado que $b_{5m+5-5k} \equiv 0 \pmod 5$.

Este teorema es sólo una de las propiedades de divisibilidad de la función partición. Los métodos de esta sección pueden usarse para probar que $p(7n+5) \equiv 0 \pmod 7$. Con la ayuda de un análisis más extenso, puede demostrarse que $p(5^k n + r) \equiv 0 \pmod{5^k}$ si $24r \equiv 1 \pmod{5^k}$, $k = 2, 3, 4, \ldots$, y todavía hay otras congruencias relacionadas a las potencias de 5. Existen congruencias algo semejantes relacionadas a las potencias de 7, pero es un hecho interesante que $p(7^k n + r) \equiv 0 \pmod{7^k}$ si $24r \equiv 1 \pmod{7^k}$ es válida para $k = 1, 2$ pero es falsa para $k = 3$. También hay propiedades de divisibilidad relaciona-

das al número 11. Una identidad típica de algunas relacionadas con las propiedades de divisibilidad es

$$\sum_{n=0}^{\infty} p(5n+4)x^n = 5\frac{\varphi(x^5)^5}{\varphi(x)^6}, \qquad |x| < 1.$$

**Problemas**

1. Escribir la fórmula de Euler como

$$\varphi(x) = \sum_{j=-\infty}^{\infty} (-1)^j x^{(3j^2+j)/2}.$$

Aplicar la fórmula de Jacobi como en el Teorema 10.13, multiplicar formalmente $x\varphi(x)\varphi(x)^3$ y verificar (10.6).

2. Obtener una congruencia semejante a la del Teorema 10.16 pero para el módulo 35, aplicando el Teorema 10.16 y $p(7n+5) \equiv 0 \pmod 7$.

# Capítulo 11

# Densidad de las sucesiones de enteros

Para facilitar la definición de lo que quiere darse a entender por densidad de una sucesión de enteros es necesario usar ciertos conceptos del análisis. En este capítulo se supone que el lector está familiarizado con las ideas del límite inferior de una sucesión de números reales y la cota inferior máxima, o infimum, de un conjunto de números reales. También, en la Sección 11.2 haremos uso del hecho de que $\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$. Estas se discuten en muchos textos, por ejemplo en el *Mathematical Analysis,* por Apostol.*

En este capítulo se consideran dos tipos comunes de densidad, densidad asintótica y densidad de Schnirelmann. La primera se discute en las Secciones 11.1 y 11.3, y la segunda en la Sección 11.4. Se definirá la densidad para un conjunto $A$ de enteros positivos distintos. Se pensará en los elementos de $A$ como si estuvieran arreglados en una sucesión de acuerdo con su magnitud,

$$(11.1) \qquad a_1 < a_2 < a_3 < \cdots,$$

y también se denotará $A$ por $\{a_i\}$. Además se usará tanto el término conjunto como el de sucesión para describir $A$. El conjunto $A$ puede ser infinito o bien finito. Es decir, puede contener un número infinito de elementos o sólo un número finito de elementos. Incluso puede ser vacío. en cuyo caso se denotará por 0. Si un entero $m$ es un elemento de $A$ se escribe $m \in A$, en caso contrario se escribe $m \notin A$. El conjunto $A$ está

* Tom M. Apostol, *Mathematical Analysis,* Addison-Wesley, 1957.

contenido en $B$, $A \subset B$ o bien $B \supset A$, si todo elemento de $A$ es un elemento de $B$. Se escribe $A = B$ si $A \subset B$ y $B \subset A$, es decir si $A$ y $B$ tienen precisamente los mismos elmentos. La unión $A \cup B$ de dos conjuntos $A$ y $B$ es el conjunto de todos los elementos $m$ tales que $m \in A$ o bien $m \in B$. La intersección $A \cap B$ de $A$ y $B$ es el conjunto de todos los $m$ tales que $m \in A$ y $m \in B$. Así, por ejemplo, $A \cup A = A \cap A = A$, $A \cup 0 = A$, $A \cap 0 = 0$. Si $A$ y $B$ no tienen elemento en común, $A \cap B = 0$, se dice que $A$ y $B$ están separados. Por complemento $\overline{A}$ de $A$ debe entenderse el conjunto de todos los enteros positivos que no son elementos de $A$. Así, $A \cap \overline{A} = 0$ y $\overline{0}$ es el conjunto de todos los enteros positivos.

## 11.1 Densidad asintótica

El número de enteros positivos en un conjunto $A$ que sean menores que o iguales a $x$ se denota por $A(x)$. Por ejemplo, si $A$ consiste de los enteros pares 2, 4, 6, . . . , entonces $A(1) = 0$, $A(2) = 1$, $A(6) = 3$, $A(7) = 3$, $A(15/2) = 3$; de hecho, $A(x) = [x/2]$ si $x \geqq 0$. Por otra parte, para cualquier conjunto $A = \{a_i\}$ se tiene $A(a_j) = j$.

**Definición 11.1** *La densidad asintótica de un conjunto A es*

$$\delta_1(A) = \liminf_{n\to\infty} \frac{A(n)}{n}.$$

*En el caso de que la sucesión $A(n)/n$ tenga un límite, se dice que $A$ tiene una densidad natural, $\delta(A)$. Así que*

$$\delta(A) = \delta_1(A) = \lim_{n\to\infty} \frac{A(n)}{n}$$

*si $A$ tiene una densidad natural. Si $A$ es una sucesión finita, es evidente que $\delta(A) = 0$.*

**Teorema 11.1** *Si $A$ es una sucesión infinita, entonces*

$$\delta_1(A) = \liminf_{n\to\infty} \frac{n}{a_n}$$

*Si $\delta(A)$ existe, entonces $\delta(A) = \lim_{n\to\infty} n/a_n$.*

*Demostración.* La sucesión $k/a_k$ es una subsucesión de $A(n)/n$ y de aquí que

$$\liminf_{n\to\infty} \frac{A(n)}{n} \leqq \liminf_{k\to\infty} \frac{k}{a_k}.$$

Si $n$ es cualquier entero $\geqq a_1$ y $a_k$ es el menor entero en $A$ que excede a $n$, entonces $a_{k-1} \leqq n < a_k$ y

$$\frac{k}{a_k} - \frac{A(n)}{n} = \frac{k}{a_k} - \frac{k-1}{n} < \frac{k}{n} - \frac{k-1}{n} = \frac{1}{n}.$$

De donde $k/a_k - A(n)/n$ tiende hacia cero conforme crece $n$, y se concluye el teorema.

**Problemas**

1. Probar que cada uno de los conjuntos siguientes tiene una densidad natural y encontrar su valor:

   *a*) el cojunto de los enteros positivos pares;
   *b*) el conjunto de los enteros positivos impares;
   *c*) los múltiplos positivos de 3;
   *d*) los enteros positivos de la forma $4k + 2$;
   *e*) todos los enteros positivos $a$ que satisfacen $a \equiv b \pmod{m}$, donde $b$ y $m > 1$ son fijos;
   *f*) el conjunto de los primos;
   *g*) el conjunto $\{ar^n\}$ con $n = 1, 2, 3, \cdots$ y fijo $a \geqq 1$, fijo $r > 1$;
   *h*) el conjunto de todos los cuadrados perfectos;
   *i*) el conjunto de todos los cubos positivos;
   *j*) el conjunto de todas las potencias positivas, esto es, todos los números de la forma $a^n$ con $a \geqq 1$, $n \geqq 2$.

2. Si la densidad natural $\delta(A)$ existe, probar que $\delta(\bar{A})$ también existe y que $\delta(A) + \delta(\bar{A}) = 1$.
3. Probar que $\delta(A)$ existe si y sólo si $\delta_1(A) + \delta_1(\bar{A}) = 1$.
4. Para cualquier conjunto $A$, probar que $\delta_1(A) + \delta_1(\bar{A}) \leqq 1$.
5. Definir $A_n$ como el conjunto de todos los $a$ tales que $(2n)! \leqq a < (2n + 1)!$ y sea $A$ la unión de todos los conjuntos $A_n$, $n = 1, 2, 3, \cdots$. Probar que $\delta_1(A) + \delta_1(\bar{A}) = 0$.
6. Sea $A^*$ el conjunto restante después de que se han eliminado un número finito de enteros de un conjunto $A$. Probar que $\delta_1(A) = \delta_1(A^*)$ y que $\delta(A)$ existe si y sólo si $\delta(A^*)$ existe.
7. Si dos conjuntos $A$ y $B$ son idénticos más allá de un entero fijo $n$, probar que $\delta_1(A) = \delta_1(B)$.
8. Dado cualquier conjunto $A = \{a_j\}$ y cualquier entero $b \geqq 0$, definir $B = \{b + a_j\}$. Probar que $\delta_1(A) = \delta_1(B)$.
9. Sea $A$ el conjunto de todos los enteros positivos pares, $B_1$ el conjunto de todos los enteros positivos pares con un número par de dígitos para la base diez, y $B_2$ el conjunto de todos los enteros positivos impares. Definir $B = B_1 \cup B_2$ y probar que $\delta(A)$ y $\delta(B)$ existen, pero que $\delta(A \cup B)$ y $\delta(A \cap B)$ no existen.
10. Si $A \cap B = 0$, probar que $\delta_1(A \cup B) \geqq \delta_1(A) + \delta_1(B)$.
11. Denotemos por $S$ cualquier conjunto finito de enteros positivos $a_1, a_2, \cdots, a_m$. Probar que el conjunto $A$ de todos los enteros positivos no divisibles entre cualquier miembro de $S$ tiene la densidad natural

$$1 - \sum_{i=1}^{m} \frac{1}{a_i} + \sum_{i<j} \frac{1}{[a_i, a_j]} - \sum_{i<j<k} \frac{1}{[a_i, a_j, a_k]} + \cdots + \frac{(-1)^m}{[a_1, a_2, \cdots, a_m]}.$$

12. Sea $A$ un conjunto de enteros positivos tales que para todo entero $m$, la ecuación $x + y = m$ tiene cuando más una solución no considerando el orden con $x$ y $y$ en $A$. Probar que $A$ tiene densidad cero. Aún más, probar que $A(n) \leqq 2\sqrt{n}$.
13. Definir $A = \{a_j\}$ del modo siguiente. Con $a_1 = 1$, definir $a_{k+1}$ como el menor entero positivo que sea diferente de todos los números $a_h + a_i - a_j$, con $1 \leqq h \leqq k$, $1 \leqq i \leqq k$, $1 \leqq j \leqq k$. Probar que $A$ satisface la desigualdad del problema anterior, y que $A(n) \geqq \sqrt[3]{n} - 1$.
14. Sea $P$ el conjunto de enteros $\{m^k\}$ con $m = 1, 2, 3, \cdots$ y $k = 2, 3, 4, \cdots$. Sea $P_1$ el subconjunto con $k = 3, 4, \cdots$. Probar que

$$\lim_{n\to\infty} \frac{P_1(n)}{P(n)} = 0.$$

15. Encontrar la densidad asintótica del conjunto de enteros positivos que tienen un número impar de dígitos en la representación de base diez.

## 11.2 Enteros exentos de cuadrados

Un entero es exento de cuadrados si no es divisible entre cuadrado perfecto $a^2 > 1$. Se probará que el conjunto de enteros exentos de cuadrados tiene la densidad natural $6/\pi^2$.

**Lema 11.2** *La función $\tau(n)$, que representa el número de divisores positivos de $n$, satisface la desigualdad $\tau(n) \leqq 2\sqrt{n}$ para $n \geqq 1$.*

*Demostración.* Considérense los divisores positivos, $d$, de $n$. Correspondiendo a cada $d \geqq \sqrt{n}$ se tiene el divisor distinto $d' = n/d$, y $1 \leqq d' \leqq \sqrt{n}$. Por tanto $\tau(n)$ no puede exceder al doble del número de divisores $d$ tales que $1 \leqq d \leqq \sqrt{n}$. Evidentemente el número de estos $d$ no puede exceder a $\sqrt{n}$ y se tiene $\tau(n) \leqq 2\sqrt{n}$.

**Teorema 11.3** *Se tiene*

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} \sum_{n=1}^{\infty} \frac{1}{n^2} = 1.$$

*Demostración.* Escribiendo

$$P_m = \sum_{n=1}^{m} \frac{\mu(n)}{n^2} \sum_{n=1}^{m} \frac{1}{n^2} = R_m S_m, \tag{11.4}$$

consideremos primero un entero fijo $j \leqq m$. Si $d$ es cualquier divisor de $j$, digamos $j = dq$, entonces $\mu(d)/d^2$ es un término de $R_m$ y $1/q^2$ es un término de $S_m$ y $\mu(d)/(dq)^2 = \mu(d)/j^2$ se encuentra en $P_m$. Entonces $1/j^2$ se encuentra en $P_m$ con coeficiente

$$\sum_{d|j} \mu(d) = \begin{cases} 1 \text{ si } j = 1 \\ 0 \text{ si } j > 1 \end{cases}$$

por el Teorema 4.6. En el caso de que $j > m$, el producto $\mu(d)/(dq)^2$ puede aparecer en $P_m$ para algunos divisores $d$ de $j$. Por tanto puede escribirse

$$P_m = \sum_{j=1}^{m} \left( \sum_{d|j} \mu(d) \right) \frac{1}{j^2} + \sum_{j=m+1}^{m^2} \left( \sum_{d|j}{}' \mu(d) \right) \frac{1}{j^2}$$

donde $\sum'$ denota una suma sobre los divisores apropiados $d$ de $j$. Así, se tiene

$$P_m - 1 = \sum_{j=m+1}^{m^2} \sum_{d|j} \frac{\mu(d)}{j^2} = \sum_{j=m+1}^{m^2} \frac{c_j}{j^2}, \qquad c_j = \sum_{d|j}{}' \mu(d),$$

y, aplicando el Lema 11.2, se observa que

$$|c_j| \leqq \sum_{d|j} |\mu(d)| \leqq \sum_{d|j} |\mu(d)| \leqq \sum_{d|j} 1 = \tau(j) \leqq 2\sqrt{j}.$$

Ahora se tiene

$$|P_m - 1| \leqq \sum_{j=m+1}^{m^2} \frac{|c_j|}{j^2} \leqq \sum_{j=m+1}^{m^2} \frac{2\sqrt{j}}{j^2} = \sum_{j=m+1}^{m^2} \frac{2}{j^{3/2}}.$$

Aplicando la condición de Cauchy a la serie convergente $\sum 2/j^{3/2}$ se ve que $|P_m - 1|$ tiende hacia cero conforme $m$ tiende al infinito. En vista de (11.4) esto establece el teorema.

**Corolario 11.4** *Se tiene*

$$\sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}.$$

*Demostración.* Es bien sabido, con base en los resultados elementales en la teoría de las series de Fourier, que $\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$. Por ejemplo, se concluye haciendo $x = 0$ en el resultado

$$\frac{x^2}{2} = \pi x - \frac{\pi^2}{3} + 2 \sum_{n=1}^{\infty} \frac{\cos nx}{n^2},$$

el cual es válido para $x$ en el intervalo $0 \leqq x \leqq 2\pi$. Este resultado se encuentra en *Mathematical Analysis* de Apostol*. Esto con el Teorema 11.3 prueba el corolario.

* Tom M. Apostol, *Mathematical Analysis,* Addison-Wesley, 1957, pág. 501.

**Teorema 11.5** *El conjunto de enteros exentos de cuadrados tienen la densidad natural* $6/\pi^2$

*Demostración.* Denotemos por $S$ a la sucesión 1, 2, 3, 5, 6, 7, 10, . . . de enteros exentos de cuadrados. Para cualquier entero positivo $n$ denotemos por $p_1 \; p_2 \; \cdots, p_r$ todos los primos tales que $p_j^2 \leqq n$. Primero se desea probar que

$$(11.5) \qquad S(n) = \sum (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_r} \left[\frac{n}{(p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r})^2}\right]$$

donde la suma recorre todos los $2^r$ términos obtenidos haciendo $\alpha_j = 0$ o bien 1. Ahora bien, $[n/t^2]$ es el número de enteros $\leqq n$ que son divisibles entre $t^2$, y puede interpretarse cada término del segundo miembro de (11.5) como una cuenta de esos enteros $m \leqq n$ que son divisibles entre $(p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_r^{\alpha_r})^2$

Si $m$ es exento de cuadrados, $1 \leqq m \leqq n$, entonces $m$ es contado por el término $[n]$ y por ningún otro término. Si $1 \leqq m \leqq n$ y $m$ es divisible entre $p_1^2$ pero no entre otro $p_j^2$, entonces $m$ es contado por los términos $[n]$ y $-[n/p_1^2]$, una vez positivamente y una vez negativamente, una cuenta neta de $1 - 1 = 0$. Para tomar el caso general, considérese un entero $m$, $1 \leqq m \leqq n$, que sea divisible entre $p_{j_1}^2, p_{j_2}^2, \cdots, p_{j_s}^2$ $s \geqq 1$, pero no entre cualquiera de los otros $p_j^2$. Entonces $m$ es contado por los términos

$$(-1)^{\alpha_{j_1}+\alpha_{j_2}+\cdots+\alpha_{j_s}} \left[\frac{n}{(p_{j_1}^{\alpha_{j_1}}p_{j_2}^{\alpha_{j_2}} \cdots p_{j_s}^{\alpha_{j_s}})^2}\right].$$

De donde la cuenta neta para este $m$ es

$$\sum (-1)^{\alpha_{j_1}+\alpha_{j_2}+\cdots+\alpha_{j_s}} = \sum (-1)^{\alpha_{j_1}} \sum (-1)^{\alpha_{j_2}} \cdots \sum (-1)^{\alpha_{j_s}} = 0$$

puesto que

$$\sum (-1)^{\alpha_j} = 1 + (-1) = 0.$$

Esta establece (11.5).

A continuación se observa que (11.5) puede escribirse como

$$(11.6) \qquad S(n) = \sum_{d|p_1p_2\cdots p_r} \mu(d) \left[\frac{n}{d^2}\right].$$

En esta suma cualquier término para el cual $d^2 > n$ tiene el factor $[n/d^2] = 0$ y puede restringirse $d$ en (11.6) en tal forma que $d^2 \leqq n$. En efecto, se tiene

$$(11.7) \qquad S(n) = \sum_{d^2 \leqq n} \mu(d) \left[\frac{n}{d^2}\right],$$

donde el $d$ recorre todos los enteros positivos tales que $d^2 \leqq n$, puesto que cualquier término en (11.7) que no está en (11.6) pertenecerá a un valor de $d$ que no es exento de cuadrados. En este caso el término tiene el factor $\mu(d) = 0$.

Aplicando el Corolario 11.4 y (11.7) se encuentra

$$S(n) - \frac{6n}{\pi^2} = \sum_{d^2 \leq n} \mu(d) \left( \left[ \frac{n}{d^2} \right] - \frac{n}{d^2} \right) - \sum_{d^2 > n} \mu(d) \frac{n}{d^2},$$

y de aquí que

$$(11.8) \qquad \left| \frac{S(n)}{n} - \frac{6}{\pi^2} \right| \leqq \frac{1}{n} \sum_{d^2 \leqq n} \left| \left[ \frac{n}{d^2} \right] - \frac{n}{d^2} \right| + \sum_{d^2 > n} \frac{1}{d^2}.$$

Pero

$$\frac{1}{n} \sum_{d^2 \leqq n} \left| \left[ \frac{n}{d^2} \right] - \frac{n}{d^2} \right| \leqq \frac{1}{n} \sum_{d^2 \leqq n} 1 \leqq \frac{1}{\sqrt{n}} \to 0 \quad \text{como } n \to \infty$$

y

$$\sum_{d^2 > n} \frac{1}{d^2} \to 0 \quad \text{como } n \to \infty$$

dado que $\sum 1/d^2$ converge. Por tanto, el segundo miembro de (11.8) tiende hacia cero y se tiene $S(n)/n \to 6/\pi^2$ conforme $n \to \infty$.

**Problemas**

1. Encontrar la densidad del conjunto de enteros que no sean divisibles entre los cuadrados $> 4$.
2. Encontrar la densidad del conjunto de enteros que no sean divisibles entre los cuadrados $> 100$.
3. Encontrar la densidad del conjunto de enteros que no sean divisibles entre los cuadrados impares $> 1$.

## 11.3 Conjuntos de densidad cero

Se necesitará el siguiente resultado bien conocido de la teoría de los productos infinitos. Por conveniencia se probará aquí.

**Lema 11.6** *Sea* $\sum c_j$ *una serie divergente con* $0 < c_j < 1$ *para* $j = 1, 2, \ldots$ . *Entonces, dado cualquier número real* $\varepsilon > 0$, *existe un entero* $N$ *tal que* $\prod_{j=1}^{n} (1 - c_j) < \varepsilon$ *para todo entero* $n \geqq N$.

*Demostración.* Se observa que

$$e^{-c_j} = (1 - c_j) + \left( \frac{c_j^2}{2!} - \frac{c_j^3}{3!} \right) + \left( \frac{c_j^4}{4!} - \frac{c_j^5}{5!} \right) \cdots > 1 - c_j$$

y de aquí que

$$\prod_{j=1}^{n} (1 - c_j) < \prod_{j=1}^{n} e^{-c_j} = e^{-\sum_{j=1}^{n} c_j}.$$

Puesto que $\sum c_j$ diverge puede escogerse $N$ de manera que

$$e^{-\sum_{j=1}^{N} c_j} < \varepsilon,$$

y se concluye el lema.

En esta sección usaremos un detalle de notación especial. Para cualquier conjunto de enteros $A$ y cualquier primo $p$, $A_p$ denotará el conjunto de aquellos elementos de $A$ tales que $p|a$ pero $p^2 \not| a$.

**Teorema 11.7** *Si existe un conjunto de primos* $\{p_i\}$ *tales que* $\sum p_i^{-1}$ *diverge y tiene densidad natural cero para* $i = 1, 2, 3, \cdots$, *entonces* $A$ *tiene densidad natural cero.*

*Demostración.* Denotemos por $I$ el conjunto de todos los enteros positivos, sea $C^{(r)} = I_{p1} \cup I_{p2} \cup \cdots \cup I_{p_r}$ y sea $B^{(r)} = \overline{C^{(r)}}$. Entonces $A \cap I_{p_i} = A_{p_i}$, $A \cap C^{(r)} = A_{p1} \cup A_{p2} \cup \cdots \cup A_{p_r}$ y de aquí que

(11.9) $$A \subset B^{(r)} \cup A_{p1} \cup A_{p2} \cup \cdots \cup A_{p_r}.$$

Ahora $B^{(r)}$ consiste de todos los enteros positivos excepto aquellos tales que $p_j|n$, $p_j^2 \not| n$ para por lo menos un $j = 1, 2, \cdots, r$ y se probará que

(11.10) $$B^{(r)}(n) = \sum (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_r} \left[\frac{n}{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}}\right]$$

donde la suma se extiende sobre los $3^r$ términos obtenidos tomando cada $\alpha_i = 0$, 1, o bien 2. La demostración es semejante a la de (11.5). Cualquier entero positivo $m \leqq n$ puede escribirse como

$$m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r} k, \qquad (k, p_1 p_2 \cdots p_r) = 1, \quad \beta_i \geqq 0.$$

Sea $\gamma_i = \beta_i$ si $\beta_i = 0$ o bien 1, y $\gamma_i = 2$ si $\beta_i \geqq 2$. Entonces $m$ es contado por los términos del segundo miembro de (11.10) para los cuales $0 \leqq \alpha_i \leqq \gamma_i$, $i = 1, 2, \cdots, r$ y es contado con el signo $(-1)^{\alpha_1+\alpha_2+\cdots+\alpha_r}$. Entonces la cuenta neta para $m$ es

$$\sum_{\alpha_1=0}^{\gamma_1} \sum_{\alpha_2=0}^{\gamma_2} \cdots \sum_{\alpha_r=0}^{\gamma_r} (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_r} = \prod_{i=1}^{r} \left( \sum_{\alpha_i=0}^{\gamma_i} (-1)^{\alpha_i} \right).$$

Pero

$$\sum_{\alpha_i=0}^{\gamma_i} (-1)^{\alpha_i} = \begin{cases} 1 & = 1 \text{ si } \gamma_i = 0 \\ 1 - 1 & = 0 \text{ si } \gamma_i = 1 \\ 1 - 1 + 1 & = 1 \text{ si } \gamma_i = 2 \end{cases}$$

y se ve que $m$ tiene una cuenta de 0 si cualquier $\gamma_i = 1$ y en cualquier otro caso tiene una cuenta de 1. Puesto que $\gamma_i = 1$ si, y sólo si, $\beta_i = 1$, el segundo miembro de (11.10) cuenta los $m \leqq n$ que estén en $B^{(r)}$, y se establece (11.10).

Quitando el símbolo de máximo entero en (11.10) se obtiene la desigualdad

$$B^{(r)}(n) \leqq \sum (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_r} \frac{n}{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}} + 3^r,$$

de aquí que

$$(11.11) \qquad \frac{B^{(r)}(n)}{n} \leqq \prod_{i=1}^{r}\left(1 - \frac{1}{p_i} + \frac{1}{p_i^2}\right) + \frac{3^r}{n}.$$

Para probar el teorema debe demostrarse que para cualquier real $\varepsilon > 0$ existe un $N$ tal que $A(n)/n < \varepsilon$ para $n \geqq N$. Primero se escoge $r$ de modo que

$$(11.12) \qquad \prod_{i=1}^{r}\left(1 - \frac{1}{p_i} + \frac{1}{p_i^2}\right) < \frac{\varepsilon}{4},$$

lo cual puede hacerse por el Lema 11.6 dado que $\sum p_i^{-1}$, y por tanto $\sum (p_i^{-1} - p_i^{-2})$ también diverge. Los conjuntos $A_{p_i}$ tienen la densidad natural cero y así puede encontrarse un entero $N_1$ tal que

$$(11.13) \qquad \frac{A_{p_i}(n)}{n} > \frac{\varepsilon}{2r}, \qquad i = 1, 2, \ldots, r$$

si $n \geqq N_1$. Tomando $N \geqq N_1$, $N \geqq 3^r \cdot 4/\varepsilon$ y aplicando (11.9), (11.11), (11.12) y (11.13) se ve que

$$\frac{A(n)}{n} \leqq \frac{B^{(r)}(n)}{n} + \prod_{i=1}^{r} \frac{A_{p_i}(n)}{n} < \frac{\varepsilon}{4} + \frac{\varepsilon}{4} + r\left(\frac{\varepsilon}{2r}\right) = \varepsilon$$

si $n \geqq N$.

**Teorema 11.8** *Sea $k$ un entero positivo fijo. Si cada entero en un conjunto $A$ es divisible entre $k$ o menos factores primos distintos, entonces $\delta(A) = 0$.*

*Demostración.* Denotemos por $D^{(k)}$ el conjunto de todos los enteros positivos que tienen $k$ o menos factores primos distintos. Entonces $A \subset D^{(k)}$, $A(n) \leqq D^{(k)}(n)$ y sólo es necesario probar el teorema para $D^{(k)}$. La demostración es por inducción sobre $k$. Para $k = 1$ el conjunto $D^{(1)}$ consiste de todas las potencias primas, $D^{(1)} = \{p^s\}$. Se aplica el Teorema 11.7, tomando los $p_i$ como todos los primos. Por el Teorema 8.2, la serie $\sum p_i^{-1}$ diverge y $\delta(D_{p_i}^{(1)}) = 0$ puesto que $D_{p_i}^{(1)}$ consiste del único elemento $p_i$. De donde $\delta(D^{(1)}) = 0$.

Volviendo al $k$ general, se supone que el teorema se cumple en el caso $k-1$. Los elementos de $D_p^{(k)}$ son los enteros positivos que son divisibles entre $p$, pero no entre $p^2$, y que tienen $k$ o menos factores primos distintos. Si $a \in D_p^{(k)}$, entonces $a/p \in D^{(k-1)}$. Por lo tanto, $D_p^{(k)}(n) \leqq D^{(k-1)}(n/p)$ y de aquí que $\delta(D^{(k-1)}) = 0$ implica $\delta(D_p^{(k)}) = 0$. Ahora puede aplicarse el Teorema 11.7 como antes y se concluye que $\delta(D^{(k)}) = 0$.

Como otra aplicación del Teorema 11.7 probaremos lo siguiente:

**Teorema 11.9** *El conjunto de enteros* $\{\phi(m)\}$, $m = 1, 2, 3, \cdots$ *tiene densidad natural cero.*

*Demostración.* Denotemos el conjunto bajo consideración por $A$. Dado $\varepsilon > 0$, se escoge $k$ de manera que $2^{-k} < \varepsilon/2$ y se divide $A$ en dos conjuntos separados $B$ y $C$, donde $B$ consiste de aquellos miembros de $A$ que sean divisibles entre $2^k$. De aquí que $B(n) \leqq 2^{-k}n$ para todo $n$.

Ahora bien, $C$ consiste de los números $\phi(m)$ de $A$ que no son divisibles entre $2^k$. Denotemos por $C^*$ el conjunto de $m$ para los cuales $\phi(m) \in C$. *Si* $q_1, q_2, \cdots, q_r$ son los factores primos distintos de $m$, entonces

$$\phi(m) = \frac{m}{q_1 q_2 \cdots q_r}(q_1 - 1)(q_2 - 1) \cdots (q_r - 1),$$

lo cual demuestra que $2^{r-1} | \phi(m)$ dado que todos excepto uno de los $q_i$ deben ser impares. Por lo tanto, si $m \in C^*$ entonces $r \leqq k$ y, digamos,

$$\phi(m) = m \prod_{i=1}^{r} \left(1 - \frac{1}{q_i}\right) \geqq m\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) \cdots \left(1 - \frac{1}{p_k}\right) = mc_k,$$

De aquí que si $\phi(m) \in C$ y $\phi(m) \leqq n$, entonces $m \leqq n/c_k$ y de donde $C(n) \leqq C^*(n/c_k)$. Pero ahora los elementos del conjunto $C^*$ tienen $k$ o menos factores primos distintos y así, por el Teorema 11.8, se ve que existe un entero $N$ tal que $C^*(m)/m < \varepsilon c_k/2$ para $m \geqq N$. Por lo tanto, $C(n) \leqq C^*(n/c_k) < \varepsilon n/2$ si $n \geqq c_k N$, y $B(n) \leqq 2^{-k}n < \varepsilon n/2$. Finalmente se tiene $A(n) = B(n) + C(n) < n\varepsilon$ si $n \geqq c_k N$ y esto implica $\delta(A) = 0$.

**Problemas**

1. Sea $k$ un entero fijo. Probar que $\delta(A) = 0$ si todo entero en $A$ tiene la forma
$$p_1 p_2 \cdots p_r p_{r+1}^{\alpha_1} p_{r+2}^{\alpha_2} \cdots p_{r+s}^{\alpha_s}$$
donde los $p_i$ son primos cualesquiera, $0 \leqq r \leqq k$, $s$ es arbitrario y $\alpha_i \geqq 2$ para $i = 1, 2, \cdots, s$.
2. Si una sucesión de enteros $A = \{a_i\}$ tiene la propiedad de que $\sum a_i^{-1}$ converge, probar que $\delta(A) = 0$. Probar que la inversa es falsa.

3. Suponiendo la proposición de que el conjunto de primos $\{q_i\}$ de la forma $4n + 3$ tiene la propiedad de que $\sum q_i^{-1}$ diverge, probar que el conjunto de enteros cada uno de los cuales es representable como una suma de dos cuadrados tiene densidad cero.

## 11.4 Densidad de Schnirelmann y el teorema $\alpha\beta$

**Definición 11.2** *La densidad de Schnirelmann $d(A)$ de un conjunto $A$ de enteros no negativos es*

$$d(A) = \inf_{n \geq 1} \frac{A(n)}{n},$$

*donde $A(n)$ es el número de enteros positivos $\leqq n$ en el conjunto $A$.*

Comparando esto con la Definición 11.1, se ve inmediatamente que $0 \leqq d(A) \leqq \delta_1(A) \leqq 1$. La densidad de Schnirelmann difiere de la densidad asintótica en que es susceptible a los primeros términos de la sucesión. En verdad, si $1 \notin A$ entonces $d(A) = 0$, si $2 \notin A$ entonces $d(A) \leqq \frac{1}{2}$, mientras que fácilmente se ve que $\delta_1(A)$ no cambia si los números 1 y 2 se quitan o se agregan a $A$. También $d(A) = 1$ si, y sólo si, $A$ contiene todos los enteros positivos.

Hasta ahora se han considerado los conjuntos $A$ que consisten sólo de enteros positivos. Sin embargo, la Definición 11.2 se ha redactado en tal forma que $A$ puede contener a 0, pero debe hacerse notar que el número 0 no es contado por $A(n)$.

**Definición 11.3** *Supóngase que $0 \in A$ y $0 \in B$. La suma $A + B$ de los conjuntos $A$ y $B$ es la colección de todos los enteros de la forma $a + b$ donde $a \in A$ y $b \in B$.*

Nótese que $A \subset A + B$, $B \subset A + B$. Como un ejemplo tomemos $S$ como el conjunto de los cuadrados $0, 1, 4, 9, \cdots$ e $I$ el conjunto de todos los enteros no negativos. Entonces, por el Teorema 5.6, se ve que $S + S + S + S = I$.

La suma $A + B$ no ha sido definida a menos que $0 \in A$ y $0 \in B$. En el resto de este capítulo se supondrá que 0 está tanto en $A$ como en $B$. No obstante, podría definirse la suma para todo $A$ y $B$ como la suma de los conjuntos obtenidos a partir de $A$ y $B$ agregando el número 0 a cada uno. Esto es equivalente a definir la suma como la colección $\{a, b, a + b\}$ con $a \in A$, $b \in B$.

El resultado que se demuestra en el resto de esta sección es el teorema $\alpha\beta$ de H. B. Mann, el cual fue conjeturado en el año de 1931 aproximadamente, con demostraciones intentadas subsecuentemente por muchos matemáticos. El teorema establece que si $A$ y $B$ son conjuntos enteros no negativos, cada uno conteniendo a 0, y si $\alpha, \beta, \gamma$ son las densidades de

Schnirelmann de $A, B, A + B$, entonces $\gamma \geqq \min(1, \alpha + \beta)$. En otras palabras, $\gamma \geqq \alpha + \beta$ a menos que $\alpha + \beta > 1$, en cuyo caso $\gamma = 1$.

Realmente se probará un resultado un poco más fuerte, Teorema 11.15, a partir del cual se deducirá el teorema $\alpha\beta$. Empecemos por considerar cualquier entero positivo $g$ y dos conjuntos $A_1$ y $B_1$ de enteros no negativos que no exceden a $g$. Se supondrá en todo el deasrrollo que $A_1$ y $B_1$ son esos conjuntos y que 0 pertenece tanto a $A_1$ como a $B_1$. Denotando $A_1 + B_1$ por $C_1$, se observa que $C_1$ puede tener elementos $> g$ aunque $A_1$ y $B_1$ no los tengan. También supondremos que para algún $\theta$, $0 < \theta \leqq 1$,

$$(11.14) \qquad A_1(m) + B_1(m) \geqq \theta m, \qquad m = 1, 2, \cdots, g$$

Nuestra idea es primero reemplazar $A_1$ y $B_1$ por dos nuevos conjuntos, $A_2$ y $B_2$, en tal forma que se cumpla (11.14) para $A_2$ y $B_2$, que $C_2 = A_2 + B_2 \subset C_1$ y que $B_2(g) < B_1(g)$.

**Lema 11.10** *Supóngase que $A_1$ y $B_1$ satisfacen* (11.14). *Si $B_1 \not\subset A_1$ entonces existen los conjuntos $A_2$ y $B_2$ con $C_2 = A_2 + B_2$ tales que $C_2 \subset C_1$, $B_2(g) < B_1(g)$* y *$A_2(m) + B_2(m) \geqq \theta m$ para $m = 1, 2, \cdots, g$.*

*Demostración.* Simplemente traslademos a $A_1$ todos los elementos de $B_1$ que no estén ya en $A_1$. Defínase $B' = B_1 \cap \overline{A}_1$, $A_2 = A_1 \cup B'$, $B_2 = B_1 \cap \overline{B'}$, donde por $\overline{A}_1$ se denota el complemento de $A_1$, ahora el conjunto de todos los enteros no negativos que no están en $A_1$. Por lo tanto, 0 pertenece tanto a $A_2$ como a $B_2$. Entonces $A_2(m) = A_1(m) + B'(m)$ y $B_2(m) = B_1(m) - B'(m)$ de donde se tiene $A_2(m) + B_2(m) = A_1(m) + B_1(m) \geqq \theta m$ para $m = 1, 2, \cdots, g$. Ahora considérese cualquier $h \in C_2$. Entonces $h = a + b$ con $a \in A_2$ y $b \in B_2$. Notando que $B_2$ está contenido tanto en $A_1$ como en $B_1$ y que $A_2 = A_1 \cup B'$, se tiene $a \in A_1$ o bien $a \in B' \subset B_1$. En el primer caso puede escribirse $h = a + b$, $a \in A_1$, $b \in B_1$; en el segundo caso $h = b + a$, $b \in A_1$, $a \in B_1$; de aquí que en ambos casos se tiene $h \in C_1$. Así se tiene $C_2 \subset C_1$. Puesto que es obvio que $B_2(g) < B_1(g)$, el lema queda demostrado.

Se obtendrá un resultado semejante para el caso $B_1 \subset A_1$, pero es un poco más complicado. Se supone $B_1(g) > 0$, lo cual implica que existe algún entero $b > 0$ en $B_1$. Entonces si $a$ es el mayor entero en $A_1$, evidentemente la suma $a + b$ no está en $A_1$. Puede haber otros pares $a \in A_1$, $b \in B_1$ tales que $a + b \notin A_1$. Denotemos por $a_0$ el menor $a \in A_1$ tal que existe un $b \in B_1$ para el cual $a + b \notin A_1$. Dado que $B_1 \subset A_1$ se ve que $a_0 \neq 0$. Antes de definir $A_2$ y $B_2$ se obtendrán dos resultados preliminares.

**Lema 11.11** *Supóngase que $A_1$ y $B_1$ satisfacen $B_1 \subset A_1$ y $B_1(g) > 0$. Definamos $a_0$ como en el párrafo anterior. Supongamos que existen los en-*

*teros $b$ y $z$ tales que $b \in B_1$ y $z - a_0 < b \leqq z \leqq g$. Entonces, para cada $a \in A_1$ tal que $a \leqq z - b$, se tiene $a + b \in A_1$ y*

$$(11.15) \qquad A_1(z) \geqq A_1(b) + A_1(z - b).$$

*Demostración.* Se tiene $a \leqq z - b < a_0$ y $a + b \leqq z \leqq g$, de aquí que $a + b \in A_1$ debido a que $a_0$ es mínimo. Ahora existen $A_1(z - b)$ enteros positivos $a$ que pertenecen a $A_1$ con $a \leqq z - b$ y para cada uno de esos $a$, el correspondiente $a + b$ también pertenece a $A_1$. Además cada uno de esos $a + b$ satisface $b < a + b \leqq z$ y de aquí que $A_1(z) - A_1(b) \geqq A_1(z - b)$ y se tiene (11.15).

**Lema 11.12** *Supóngase que $A_1$ y $B_1$ satisfacen* (11.14), *$B_1 \subset A_1$ y $B_1(g) > 0$. Definir $a_0$ como en los párrafos anteriores. Si existe un entero $y \leqq g$ tal que $A_1(y) < \theta y$, entonces $y > a_0$.*

*Demostración.* Sea $z$ el menor entero tal que $A_1(z) < \theta z$. Entonces $y \geqq z \geqq 1$. Supuesto que $A_1(z) + B_1(z) \geqq \theta z$ se tiene $B_1(z) > 0$, y de aquí que existe un $b \in B_1$ tal que $0 < b \leqq z \leqq g$. Si $z \leqq a_0$, se tendría $z - a_0 < b \leqq z \leqq g$ y se podría aplicar el Lema 11.11 para obtener $A_1(z) \geqq A_1(b) + A_1(z - b)$. Ahora bien, $b \in B_1 \subset A_1$, de modo que se tiene $A_1(b) = A_1(b - 1) + 1 \geqq \theta(b - 1) + 1$ puesto que $b - 1 < z$. También $A_1(z - b) \geqq \theta(z - b)$, y se ha llegado a la contradicción $A_1(z) \geqq \theta(b - 1) + 1 + \theta(z - b) = \theta(z - 1) + 1 \geqq \theta z$. Por tanto se tiene $z > a_0$ y de aquí que $y > a_0$.

**Lema 11.13** *Supongamos que $A_1$ y $B_1$ satisfacen $B_1 \subset A_1$ y $B_1(g) > 0$. Denotemos por $B'$ el conjunto de todos los $b \in B_1$ tales que $a_0 + b \notin A_1$, y denotemos por $A'$ el conjunto de todos los enteros $a_0 + b$ tales que $b \in B'$ y $a_0 + b \leqq g$. Finalmente, considérese $A_2 = A_1 \cup A'$ y $B_2 = B_1 \cap \overline{B'}$. Entonces $C_2 \subset C_1$ y $B_2(g) < B_1(g)$.*

*Demostración.* Nótese que $0 \in A_2$ y $0 \in B_2$, de modo que la suma $C_2$ está bien definida. Si $h \in C_2$, entonces $h = a + b$, $a \in A_1 \cup A'$, $b \in B_1 \cap \overline{B'}$. Si $a \in A_1$, entonces $h = a + b \in C_1$, supuesto que $a \in A_1$, $b \in B_1$. Si $a \in A'$, entonces $a = a_0 + b_1$ para algún $b_1 \in B'$, y se tiene $h = a_0 + b + b_1$. Aquí $a_0 + b \in A_1$ puesto que de otra manera se tendría $b \in B'$. Puesto que $b_1 \in B_1$, nuevamente se tiene $h \in C_1$. Finalmente, $B_2(g) < B_1(g)$, puesto que la definición de $a_0$ asegura que $B'(g) < 0$.

**Lema 11.14** *Para $A_1$, $B_1$, $A_2$, $B_2$, como en el Lema* 11.13, *si $A_1$, $B_1$ satisfacen* (11.14) *entonces*

$$(11.16) \qquad A_2(m) + B_2(m) \geqq \theta m \quad \textit{para } m = 1, 2, \ldots, g.$$

*Demostración.* Con base en la forma en que se escogieron $A'$, $B'$, $A_2$, $B_2$, se tiene

$$\begin{aligned}A_2(m) &= A_1(m) + A'(m),\\ B_2(m) &= B_1(m) - B'(m),\\ A'(m) &= B'(m - a_0),\\ A_2(m) + B_2(m) &= A_1(m) + B_1(m) - (B'(m) - B'(m - a_0)),\end{aligned}$$

para $m = 1, 2, \ldots, g$. Por lo tanto se cumple (11.16) para todo $m$ para el cual $B'(m) = B'(m - a_0)$. Considérese cualquier $m \leqq g$ para el cual $B'(m) > B'(m - a_0)$. Entonces $B_1(m) - B_1(m - a_0) \geqq B'(m) - B'(m - a_0) > 0$ y denotemos por $b_0$ el menor elemento de $B_1$ tal que $m - a_0 < b_0 \leqq m$. Por lo tanto

$$\begin{aligned}(11.17)\quad A_2(m) + B_2(m) &\geqq A_1(m) + B_1(m) - (B_1(m) - B_1(m - a_0))\\ &= A_1(m) + B_1(m - a_0)\\ &= A_1(m) + B_1(b_0 - 1).\end{aligned}$$

Ahora $m - a_0 < b_0 \leqq m \leqq g$, de modo que puede aplicarse el Lema 11.11 con $b = b_0$ y $z = m$ para obtener

$$A_1(m) \geqq A_1(b_0) + A_1(m - b_0).$$

También se tiene $m - b_0 < a_0$ de modo que el Lema 11.12 demuestra que

$$A_1(m - b_0) \geqq \theta(m - b_0).$$

Así que (11.17) puede reducirse a

$$A_2(m) + B_2(m) \geqq A_1(b_0) + \theta(m - b_0) + B_1(b_0 - 1).$$

Pero $b_0 \in B_1 \subset A_1$, así que se tiene $A_1(b_0) = A_1(b_0 - 1) + 1$. Aplicando esto y (11.14) se tiene

$$\begin{aligned}A_2(m) + B_2(m) &\geqq A_1(b_0 - 1) + B_1(b_0 - 1) + 1 + \theta(m - b_0)\\ &\geqq \theta(b_0 - 1) + 1 + \theta(m - b_0)\\ &\geqq \theta m.\end{aligned}$$

**Teorema 11.15** *Para cualquier entero positivo $g$, denotemos por $A_1$ y $B_1$ dos conjuntos fijos de enteros no negativos $\leqq g$. Supongamos que* 0 *pertenece a ambos conjuntos $A_1$ y $B_1$, y escribamos $C_1$ por $A_1 + B_1$. Si para algún $\theta$ tal que* $0 < \theta \leqq 1$.

$$A_1(m) + B_1(m) \geqq \theta m, \quad m = 1, 2, \ldots, g,$$

*entonces $C_1(g) \geqq \theta g$.*

*Demostración.* Si $B_1(g) = 0$, entonces $B_1$ consiste del único entero 0, $C_1 = A_1$ y $C_1(g) = A_1(g) = A_1(g) + B_1(g) \geqq \theta g$. Se probará el teorema para los conjuntos generales por inducción matemática. Supóngase que $k \geqq 1$ y que el teorema es verdadero para todo $A_1$, $B_1$, con

$B_1(g) < k$. Si $A_1(m) + B_1(m) \geqq \theta m$ para $m = 1, 2, \cdots, g$ y si $B_1(g) = k$, entonces el Lema 11.10 o bien los Lemas 11.13 y 11.14 nos proporcionan los conjuntos $A_2$, $B_2$ tales que $B_2(g) < k$, $C_2 \subset C_1$ y $A_2(m) + B_2(m) \geqq \theta m$ para $m = 1, 2, \cdots, g$. Por lo tanto, por nuestra hipótesis de inducción, se tiene $C_2(g) \geqq \theta g$, lo cual implica $C_1(g) \geqq \theta g$.

**Teorema 11.16** *El teorema $\alpha\beta$. Sean $A$ y $B$ conjuntos cualesquiera de enteros no negativos, cada uno conteniendo a 0 y denotemos por $\alpha$, $\beta$, $\gamma$ las densidades de Schnirelmann de $A$, $B$, $A + B$ respectivamente. Entonces $\gamma \geqq \text{mín}\ (1, \alpha + \beta)$.*

*Demostración.* Supóngase que $A_1$ y $B_1$ consisten de los elementos de $A$ y $B$, respectivamente, que no exceden a $g$, un entero positivo arbitrario. Entonces $A_1(m) \geqq \alpha m$ y $B_1(m) \geqq \beta m$ para $m = 1, 2, \cdots, g$. Si se toma $\theta = \text{mín}\ (1, \alpha + \beta)$, se satisfacen las condiciones del Teorema 11.15 y se concluye que $C_1(g) \geqq \theta g$. Puesto que $C_1(g) \geqq \theta g$ para todo entero positivo $g$, se tiene $\gamma \geqq \theta = \text{mín}\ (1, \alpha + \beta)$.

**Problemas**

1. ¿Cuál es la densidad de Schnirelmann del conjunto de enteros impares positivos? ¿Del conjunto de enteros pares positivos? ¿Del conjunto de enteros positivos $\equiv 1 \pmod 3$? ¿Del conjunto de enteros positivos $\equiv 1 \pmod m$?
2. Probar que el análogo del Teorema 11.1 para la densidad de Schnirelmann, a saber, $d(A) = \inf n/a_n$ es falso.
3. Probar que el análogo del Teorema 11.16 para la densidad asintótica es falso. *Sugerencia*: tomar $A$ como el conjunto de todos los enteros positivos pares y considérese $A + A$.
4. Probar que si $d(A) = \alpha$, entonces $A(n) \geqq \alpha n$ para todo entero positivo $n$. Probar que el análogo de esto para la densidad asintótica es falso.
5. Establecer que el Teorema 11.16 no implica el Teorema 11.15 considerando los conjuntos $A = \{0, 1, 2, 4, 6, 8, 10, \cdots\}$, $B = \{0, 2, 4, 6, 8, 10, \cdots\}$. El Teorema 11.16 afirma que la densidad de $A + B$ es $\geqq \frac{1}{2}$, mientras que el Teorema 11.15 dice mucho más.
6. Presentar dos conjuntos $A$ y $B$ tales que $d(A) = d(B) = 0$, $d(A + B) = 1$.
7. Para dos conjuntos cualesquiera $A$ y $B$ de enteros no negativos, escribir $\alpha = d(A)$, $\beta = d(B)$, $\gamma = d(A + B)$. Probar que $\gamma \geqq \alpha + \beta - \alpha\beta$.
8. Considerar un conjunto $A$ con densidad de Schnirelmann positiva. Probar que para algún entero positivo $n$

$$nA = (n+1)A = (n+2)A = \cdots = I,$$

donde $I$ es el conjunto de todos los enteros no negativos y $nA = A + A + \cdots + A$ con $n$ sumandos.

# Referencias generales


J. W. S. Cassels, *An Introduction to Diophantine Approximation,* Cambridge Tract 45, 1957.

Harvey Cohn, *A Second Course in Number Theory,* Nueva York, John Wiley and Sons, 1962.

H. Davenport, *The Higher Arithmetic,* Londres, Hutchinson's University Library, 1952.

L. E. Dickson, *History of the Theory of Numbers,* Washington, Carnegie Institution of Washington, 1919; reimpresión, Nueva York, Chelsea, 1950.

L. E. Dickson, *Introduction to the Theory of Numbers,* Chicago, University of Chicago Press, 1929.

L. E. Dickson, *Modern Elementary Theory of Numbers,* Chicago, University of Chicago Press, 1939.

G. H. Hardy y E. M. Wright, *An Introduction to the Theory of Numbers,* Cuarta edición, Oxford, Clarendon Press, 1960.

B. W. Jones, *The Arithmetic Theory of Quadratic Forms,* Carus Monograph 10, Nueva York, John Wiley and Sons, 1950.

D. H. Lehmer, *Guide to Tables in the Theory of Numbers,* Washington, Boletín, National Research Council, No. 105, 1941.

W. J. LeVeque, *Topics in Number Theory,* volúmenes I y II, Reading, Mass., Addison-Wesley, 1956.

T. Nagell, *Introduction to Number Theory,* Nueva York, John Wiley and Sons, 1951.

Ivan Niven, *Irrational Numbers,* Carus Monograph 11, Nueva York, John Wiley and Sons, 1956.

O. Ore, *Number Theory and its History,* Nueva York, McGraw-Hill, 1949.

Hans Rademacher, *Lectures on Elementary Number Theory,* Nueva York, Blaisdell Publishing Company, 1964.

J. V. Uspensky y M. H. Heaslet, *Elementary Number Theory,* Nueva York, McGraw-Hill, 1939.

I. M. Vinogradov, *Elements of Number Theory,* traducción de la quinta edición en ruso, Nueva York, Dover, 1954.

# Referencias especiales


## Capítulo 2

D. N. Lehmer, "On the congruences connected with certain magic squares", *Trans. Amer. Math. Soc.*, **31,** 529-551 (1929).

## Capítulo 5

J. Hunter, *Number Theory,* Edinburgh, Oliver and Boyd, 1964.
L. J. Mordell, "On the equation $ax^2 + by^2 - cz^2 = 0$", *Monatsh. Mathk,* Bd. **55,** 323-327 (1951).
Th. Skolem, "A simple proof of the solvability of the Diophantine equation $ax^2 + by^2 - cz^2 = 0$", *Norsk Vid. Selsk. Forh.,* Trondheim **24,** 102-107 (1952).
H. S. Vandiver, "Fermat's last theorem, its history, and the nature of the known results concerning it," *Amer. Math. Monthly,* **53,** 555-578 (1946).

## Capítulo 9

Harry Pollard, *The Theory of Algebraic Numbers,* Carus Monograph 9, Nueva York, John Wiley and Sons, 1950.
Abraham Robinson, *Numbers and Ideals,* San Francisco, Holden-Day, 1965.

## Capítulo 10

S. Ramanujan, *Collected Papers,* Cambridge Press, 1927.

## Capítulo 11

E. Artin y P. Scherk, "On the sums of two sets of integers," *Ann. Math.* (2) **44**, 138-142 (1943).
F. J. Dyson, "A theorem on the densities of sets of integers," *J. London Math. Soc.* **20,** 8-14 (1945).
H. B. Mann, "A proof of the fundamental theorem on the density of sums of sets of positive integers," *Ann. Math.* (2) **43,** 523-527 (1942).

# Respuestas

## Sección 1.2

1. *a*) 77, *b*) 1, *c*) 7, *d*) 1.
2. $g = 17$, $x = 71$, $y = -36$.
3. *a*) $x = 9$, $y = -11$, *b*) $x = 31$, $y = 44$, *c*) $x = 3$, $y = -2$. *d*) $x = 7$, $y = 8$, *e*) $x = 1$, $y = 1$, $z = -1$.
4. *a*) 3374 *b*) 3660.
5. 128.
7. 6, 10, 15.
17. 1; $n(n+1)$.
18. *a*; *b*.
25. $x = 100n + 5$, $y = 95 - 100n$, $n = 1, 2, \cdots$, lo harán.
27. $a = 10$, $b = 100$ es una solución en los enteros positivos. Todas las soluciones están dadas por $a = \pm 10$, $b = \pm 100$; $a = \pm 20$, $b = \pm 50$; $a = \pm 100$ $b = \pm 10$; $a = \pm 50$, $b = \pm 20$; con todos los arreglos de signos. Hay 16 soluciones en total.
28. $a = 10$, $b = 100$, $c = 10$, 20, 50 o bien 100; $a = 20$, $b = 50$ $c = 10$, 20, 50 o bien 100; y todas las permutaciones de éstas, 36 respuestas en total.

## Sección 1.3

16. $p$, $p^2$; $p$, $p^2$, $p^3$; $p^2$, $p^3$.
17. $p^3$, $p$.
18. $2|\alpha_j$; $3|\alpha_j$; $\alpha_j \leqq \beta_j$; $\alpha_j \leqq \beta_j$; para todo $j$, $1 \leqq j \leqq r$ en cada parte.
24. Contraejemplos para proposiciones falsas son
    (1) $a = 2$, $b = 6$, $c = 10$.
    (8) $a = 8$, $c = 4$.
    (10) $p = 5$, $a = 2$, $b = 1$, $c = 3$.
    (13) $a = 2$, $b = 5$.
25. Todo $n$ que no sea de la forma $p - 1$, es un primo impar.
39. $a, a, \cdots, a$ o bien $a, a, \cdots, 2a, 3a$.

## Sección 2.1

1. 7, 24, 41, 58, 75, 92.
2. 0, 18, 36, 3, 21, 39, 6, 24, 42, 9, 27, 45, 12, 30, 48, 15, 33.

3. 1, 5, 7, 11 (mod 12); 1, 7, 11, 13, 17, 19, 23, 29 (mod 30).
4. $y \equiv 1 \pmod 2$; $z \equiv 1 \pmod 6$.
5. $x \equiv 5 \pmod{12}$.
10. $m = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.$
    $\phi(m) = 1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4.$
11. $x = 5$.
13. 1, 9, 3, 81, 243, 27.
14. $x = 9 + 11j$.
16. $a = 2, 3, 4, 5, 6, 7, 8, 9, 10.$
    $x = 6, 4, 3, 9, 2, 8, 7, 5, 10.$
25. 1.
26. 6.
27. 0, 1.
35. Las soluciones primitivas con $a \leqq b \leqq c$ son $a = b = 1$, $c$ cualquier enterc positivo.
36. Las soluciones tales que $(a, b, c) = 1$, $c \geqq |b| \geqq |a|$ son
    $a = -b = \pm 1$, $c = 1$ o bien 2;
    $a = -1$, $b = 2$, $c = 3$;
    $a = b = \pm 1$ con cualquier $c > 0$;
    $a = 1$, $b = 1 - c$ con cualquier $c > 2$;
    $a = 2$, $b = -2n + 1$, $c = 2n + 1$ con cualquier $n > 1$.

## Sección 2.2

4. $x(x + 1)(x + 2) \cdots (x + m - 1) \equiv 0 \pmod m$.

## Sección 2.3

1. *a*) no hay solución.
   *b*) no hay solución.
   *c*) $x \equiv -82 \pmod{400}$.
2. *a*) 5. *b*) 0, *c*) 5.
3. $x = 106$.
4. $23 + 30j$.
5. $x \equiv 33 \pmod{84}$.
6. $60j - 2$.
7. $\frac{73}{105}, \frac{4}{7}$.
12. $x \equiv 42 \pmod{125}$.

## Sección 2.4

1. 1, 2.
2. 960.
3. 2640.
4. 1920.

5. 6720.
10. $n$ impar.
11. $n$ par.
12. $n = 5^k$, $k = 1, 2, \cdots$ serán.
13. 35, 39, 45, 52, 56, 70, 72, 78, 84, 90.
15. 3, 1, 2, 4.

## Sección 2.5

1. $x \equiv 1, 2, 6 \pmod 9$
   $x \equiv 1, 3 \pmod 5$
   $x \equiv 1, 6, 11, 28, 33, 38 \pmod{45}$.
2. No hay solución.
3. $x \equiv 1, 3, 5 \pmod{508}$.
4. $x \equiv 1, 3, 5, 14, 16, 27, 122, 133, 135 \pmod{143}$.

## Sección 2.6

6. No hay solución.
7. $x \equiv 4 \pmod{5^3}$.
8. $x \equiv 7, 15, 16, 24 \pmod{36}$.
9. $x \equiv 15 \pmod{3^3}$.
10. No hay solución.
11. $x \equiv 23 \pmod{7^3}$.

## Sección 2.7

1. *a*) $x^5 + x^2 + 5 \equiv 0 \pmod 7$,
   *b*) $x^2 + 3x - 2 \equiv 0 \pmod 7$.
   *c*) $x^4 - x^3 - 4x + 3 \equiv 0 \pmod 7$.

## Sección 2.8

1. *a*) $(4x + 1)^2 \equiv 2 \pmod 5$
   *b*) $(x + 1)^2 \equiv 4 \pmod 7$
   *c*) $(4x + 7)^2 \equiv 8 \pmod{11}$
   *d*) $(2x + 1)^2 \equiv 5 \pmod{13}$.

## Sección 2.9

1. 2, 2, 3, 2, 2.
2. 5.
3. 4.
4. 1, 3, 6, 3, 6, 2.
   1, 10, 5, 5, 5, 10.
7. $p - 1$. 0.
8. (*a*) 4, (*b*) 0, (*c*) 4, (*d*) 1.
9. $x^2 \equiv 1$, $x^2 \equiv 2$, $x^2 \equiv 4$, $x^2 \equiv 8$, $x^2 \equiv 9$, $x^2 \equiv 13$, $x^2 \equiv 15$, $x^2 \equiv 16 \pmod{17}$

## Sección 2.10

1. (*a*), (*e*), (*f*), (*h*), (*i*).

3.

| | 7 | −2 | 17 | 30 | 8 | 3 |
|---|---|---|---|---|---|---|
| 7 | 8 | 17 | 30 | 7 | 3 | −2 |
| −2 | 17 | 8 | 3 | −2 | 30 | 7 |
| 17 | 30 | 3 | −2 | 17 | 7 | 8 |
| 30 | 7 | −2 | 17 | 30 | 8 | 3 |
| 8 | 3 | 30 | 7 | 8 | −2 | 17 |
| 3 | −2 | 7 | 8 | 3 | 17 | 30 |

| | 1 | 4 | 5 | 0 | 2 | 3 |
|---|---|---|---|---|---|---|
| 1 | 2 | 5 | 0 | 1 | 3 | 4 |
| 4 | 5 | 2 | 3 | 4 | 0 | 1 |
| 5 | 0 | 3 | 4 | 5 | 1 | 2 |
| 0 | 1 | 4 | 5 | 0 | 2 | 3 |
| 2 | 3 | 0 | 1 | 2 | 4 | 5 |
| 3 | 4 | 1 | 2 | 3 | 5 | 0 |

## Sección 2.11

6. 8.

13.

| ⊕ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

| ⊙ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

23. 0, 1, 6, 10, 15, 16, 21, 25.
0, 2, 3, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28.

24. (*a*) y (*c*) son dominios enteros; (*b*) es un dominio entero si y sólo si *m* es primo.

## Sección 3.1

1. 1, −2, 3, −7, 0.

4. $\left(\frac{-1}{11}\right) = -1, \left(\frac{-1}{13}\right) = +1, \left(\frac{-1}{17}\right) = +1,$
$\left(\frac{2}{11}\right) = -1, \left(\frac{2}{13}\right) = -1, \left(\frac{2}{17}\right) = +1,$
$\left(\frac{-2}{11}\right) = +1, \left(\frac{-2}{13}\right) = -1, \left(\frac{-2}{17}\right) = +1,$
$\left(\frac{3}{11}\right) = +1, \left(\frac{3}{13}\right) = +1, \left(\frac{3}{17}\right) = -1.$

5. $x \equiv \pm 1 \pmod{11}$, $x \equiv \pm 5 \pmod{11}$, $x \equiv \pm 2 \pmod{11}$,
$x \equiv \pm 4 \pmod{11}$, $x \equiv \pm 3 \pmod{11}$.
$x \equiv \pm 1 \pmod{11^2}$, $x \equiv \pm 27 \pmod{11^2}$, $x \equiv \pm 2 \pmod{11^2}$,
$x \equiv \pm 48 \pmod{11^2}$, $x \equiv \pm 3 \pmod{11^2}$.

6. 1, 2, 4 (mód 7), ±1, ±3, ±4 (mód 13), ±1, ±2, ±4, ±8 (mód 17), ±1, ±4, ±5, ±6, ±7, ±9, ±13 (mód 29), ±1, ±3, ±4, ±7, ±9, ±10, ±11, ±12, ±16 (mód 37).

7. (*d*) 2, (*h*) 2.
8. (*a*) 2, (*b*) 0, (*c*) 4, (*d*) 0, (*e*) 2, (*f*) 0.

## Sección 3.2

4. (*b*), (*c*), (*d*), (*e*), (*f*).
5. $\left(\frac{7}{227}\right) = +1, \left(\frac{7}{229}\right) = -1, \left(\frac{7}{1009}\right) = +1,$
$\left(\frac{11}{227}\right) = +1, \left(\frac{11}{229}\right) = +1, \left(\frac{11}{1009}\right) = -1,$
$\left(\frac{13}{227}\right) = -1, \left(\frac{13}{229}\right) = -1, \left(\frac{13}{1009}\right) = -1.$
6. Sí.
7. $p = 2$, $p = 11$, y $p \equiv 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 \pmod{44}$.
8. $p \equiv \pm 1, \pm 3, \pm 9, \pm 13 \pmod{40}$.
9. Primos impares $p \equiv 2, 3 \pmod 5$
10. $p \equiv 1, 3 \pmod 8$.

## Sección 3.3

1. $\left(\frac{-23}{83}\right) = -1, \left(\frac{51}{71}\right) = -1, \left(\frac{71}{73}\right) = +1, \left(\frac{-35}{97}\right) = +1.$
2. (*b*).
3. (*c*).
10. $p = 2$ y $p \equiv 1 \pmod 4$.
11. 2 y $p^a$ para $p \equiv 1 \pmod 4$ y $a = 1, 2, 3, \cdots$
12. $n = 2^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ $a_1 = 0$ ó 1, $p_j \equiv 1 \pmod 4$, $a_j = 1, 2, 3 \cdots$

## Sección 4.1

1. 529, 263, 263, 263, 87.
2. 24.
3. *a*) todo $x$ tal que $x - [x] < \frac{1}{2}$,
   *b*) todo $x$,
   *c*) todos los enteros
   *d*) todo $x$ tal que $x - [x] \geqq \frac{1}{2}$,
   *e*) todo $x$ tal que $1 \leqq x < 10/9$.
5. *a*)
$$e = \begin{cases} \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] \text{ si } p \text{ es impar} \\ n + \sum_{i=1}^{\infty} \left[\frac{n}{2^i}\right] \text{ si } p = 2, \end{cases}$$
(*b*)
$$e = \begin{cases} \sum_{i=1}^{\infty} \left(\left[\frac{2n}{p^i}\right] - \left[\frac{n}{p^i}\right]\right) \text{ si } p \text{ es impar} \\ 0 \text{ si } p = 2. \end{cases}$$

## Sección 4.2

1. 7.
2. 12.
3. 2, 1, 12, 24.
4. 6.

8. $\sigma_k(p_1^{e_1}\cdots p_r^{e_r}) = \prod_{i=1}^{r} \dfrac{p_i^{k(e_i+1)}-1}{p_i^k-1}$.

10. $f(n) = n$ lo hará.

13. $x = p^{n-1}$ lo harán, donde $p$ es cualquier primo.

16. 6, 28, 496.

## Sección 4.3

1. $n = 33$ será.
3. 1.
7. $\sum_{d|n} \mu(d)\sigma(d) = (-1)^k p_1 p_2 \cdots p_k$.

## Sección 4.4

1. $x_n = a^n x_0$.
   $x_n = \begin{cases} b^{n/2}x_0 & \text{si } n \text{ es par,} \\ b^{(n-1)/2}x_1 & \text{si } n \text{ es impar.} \end{cases}$
2. $x_n = n$. $x_n = 1$. $x_n = (3^n - (-1)^n)/4$. $x_n = (3^n + (-1)^n)/2$.
3. 0, 1, 1, 2, 3, 5, 8, 13,
   21, 34.

11. *b*) $-[-n/3]$ si $n$ es impar.
    *d*) $S_3 = \{1\}$, $S_9 = \{2, 3, 5, 7\}$.

12.
| $n =$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $f(n) =$ | 0 | 1 | 2 | 4 | 6 | 9 | 12 | 16 | 20 | 25 |

$f(5+3) - f(5-3) = f(8) - f(2) = 16 - 1 = 15 = 5 \cdot 3$, por ejemplo.

13. $x_n = 1 + 2^{n-2} - (-2)^{n-2} = \begin{cases} 1 & \text{si } n \text{ es par,} \\ 1 + 2^{n-1} & \text{si } n \text{ es impar.} \end{cases}$

## Sección 5.2

2. $x = 1 + 7t$, $y = -1 + 10t$.
9. $(b_1 - b_2, c_1 - c_2) | (d_1 - d_2)$.

## Sección 5.3

1. *a*) $x = 8, y = 4$; $x = 5$, $y = 9$; $x = 2$, $y = 14$.
   *b*) $x = 6, y = 3$.
   *c*) $x = 2, y = 7$.
   *d*) $x = 2, y = 5$.
   *e*) no hay solución.
   *f*) no hay solución.
   *g*) no hay solución.

10. $ab$.

## Sección 5.4

1. *a*) $x = 1 + u,\ y = -2u + 3v,\ z = u - 2v,$
   *b*) $x = 10 + u,\ y = -2u + 3v,\ z = u - 2v,$
   *c*) $x = 1 + 2t,\ y = 6 + 15t - 2v,\ z = -2 - 5t + v,$
   *d*) $x = 2 + 2t,\ y = 15t - 2v,\ z = -5t + v,$
   *e*) $x = t,\ y = -11 + 3t + 5v,\ z = -11 + 3t + 6v.$
   *f*) no hay solución.

## Sección 5.5

1. $x = 3,\ y = 4,\ z = 5,$ $x = 4,\ y = 3,\ z = 5,$
   $x = 15,\ y = 8,\ z = 17,$ $x = 8,\ y = 15,\ z = 17,$
   $x = 5,\ y = 12,\ z = 13,$ $x = 12,\ y = 5,\ z = 13,$
   $x = 21,\ y = 20,\ z = 29,$ $x = 20,\ y = 21,\ z = 29,$
   $x = 7,\ y = 24,\ z = 25.$ $x = 24,\ y = 7,\ z = 25.$
3. *a*) $x = 3k,\ y = 4k,\ z = 5k,$
   $x = 4k,\ y = 3k,\ z = 5k.$
   *b*) ninguna.
5. $n \equiv 0, 1, 3 \pmod 4$.

## Sección 5.10

1. $N(100) = 12,\ P(100) = 0,\ Q(100) = 0,$
   $N(101) = 8,\ P(101) = 2,\ P(101) = 8,$
   $N(102) = 0,\ P(102) = 0,\ Q(102) = 0.$

## Sección 5.13

1. *a*) todo $n = 2^e p_1^{e_1}, \cdots p_k^{e_k},\ e \geq 1\ e_i$ par si $p_i \equiv 3 \pmod 4$.
   *b*) todo $n \equiv 0, 2, 6, \pmod 8$.
   *c*) todos los enteros.
   *d*) todos los enteros pares no negativos.
2. Todos los cuadrados perfectos.
9. *a*) $x = 2,\ y = -3,$ $x = -2, y = 3,$
   $x = 4,\ y = -1,$ $x = -4,\ y = 1,$
   $x = 6,\ y = -5,$ $x = -6,\ y = 5,$
   $x = 8,\ y = -5,$ $x = -8,\ y = 5.$
   *b*) no hay solución.
10. 1.

## Sección 5.14

2. *a*) $x^2 + xy + 3y^2,$ *c*) $2x^2 + xy + 6y^2,$
   *b*) $x^2 + xy + 2y^2,$ *d*) $x^2 + xy + 3y^2.$
4. $x^2 + xy + 5y^2.$

## Sección 6.1

6. $a = b = d = 1,\ c = 0$ serán.

## Sección 7.1

1. $17/3 = \langle 5, 1, 2\rangle$, $3/17 = \langle 0, 5, 1, 2\rangle$, $8/1 = \langle 8\rangle$.
3. $\langle 2,1,4,\rangle = 14/5$, $\langle -3, 2, 12\rangle = -63/25$, $\langle 0, 1, 1, 100\rangle = 101/201$.

## Sección 7.2

1. Las condiciones siguientes son necesarias y suficientes. En el caso de que $a_j = b_j$ para $0 \leqq j \leqq n$, entonces $n$ debe ser par. De otra manera, definir $r$ como el menor valor de $j$ tal que $a_j \neq b_j$. En el caso de que $r \leqq n - 1$, entonces para $r$ par se requiere $a_r < b_r$, pero para $r$ impar, $a_r > b_r$. En el caso de que $r = n$, entonces para $n$ par se requiere $a_n < b_n$, pero para $n$ impar se requiere $a_n > 1 + b_n$ o bien $a_n = 1 + b_n$ con $b_{n+1} > 1$.

## Sección 7.3

1. $(1 + \sqrt{5})/2$.
2. $(3 + \sqrt{5})/2$, $(25 - \sqrt{5})/10$.
3. *a*) $1 + \sqrt{2}$, *b*) $(1 + \sqrt{3})/2$, *c*) $1 + \sqrt{3}$, *d*) $3 - \sqrt{3}$.
4. $h_n/h_{n-1} = \begin{cases} \langle a_n, a_{n-1}, \cdots, a_2, a_1, a_0\rangle \text{ si } a_0 \neq 0, \\ \langle a_n, a_{n-1}, \cdots, a_4, a_3, a_2\rangle \text{ si } a_0 = 0. \end{cases}$

## Sección 7.4

1. $\sqrt{2} = \langle 1, 2, 2, 2, \cdots\rangle$, $\sqrt{2} - 1 = \langle 0, 2, 2, 2, \cdots\rangle$,
   $\sqrt{2}/2 = \langle 0, 1, 2, 2, 2, \cdots\rangle$
   $\sqrt{3} = \langle 1, 1, 2, 1, 2, 1, 2, \cdots\rangle$, $\frac{1}{\sqrt{3}} = \langle 0, 1, 1, 2, 1, 2, 1, 2, \cdots\rangle$.

## Sección 7.6

1. 1/1, 3/2 serán.
2. 3/1, 22/7 serán.

## Sección 7.7

1. $c = 1, 2, \cdots, 2[\sqrt{d}]$.

## Sección 8.2

1. log 9 (base 10).

## Sección 8.3

5. 1, 2, 3, 4, 6, 8, 12, 18,
   24, 30.

## Sección 9.2

1. $x - 7$, $x^3 - 7$, $x^3 - 3x^2/2 + 3x/4 - 1$, $x^4 - 4x^3 - 4x^2 + 16x - 8$.
   $7$, $\sqrt[3]{7}$, $1 + \sqrt{2} + \sqrt{3}$ son enteros algebraicos.

## Sección 9.4

3. Sí; no, por ejemplo $\alpha = \frac{1}{2}(1 + i\sqrt{3})$.

## Sección 9.5

6. $\alpha = (1 + 7i)/5$ lo será.
7. La sugerencia también es buena en el caso de que $m = -2$. Los otros casos especiales pueden manejarse mediante números tales como:
   $$\frac{1 + 4\sqrt{-3}}{7}, \frac{9 + 4\sqrt{2}}{7}, \frac{27 + \sqrt{3}}{11}, \frac{4 + 10\sqrt{5}}{11}.$$

## Sección 10.4

1. $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.$
   $p(n) = 1, 2, 3, 5, 7, 11, 15, 22, 30, 42, 56, 77.$
   $n = 13, 14, 15, 16, 17, 18, 19, 20.$
   $p(n) = 101, 135, 176, 231, 297, 385, 490, 627.$
2. $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.$
   $\sigma(n) = 1, 3, 4, 7, 6, 12, 8, 15, 13, 18, 12, 28.$
   $n = 13, 14, 15, 16, 17, 18, 19, 20.$
   $\sigma(n) = 14, 24, 24, 31, 18, 39, 20, 42.$

## Sección 10.6

2. $p(35m + 19) \equiv 0 \pmod{35}$.

## Sección 11.1

1. *a)* $\frac{1}{2}$, *b)* $\frac{1}{2}$, *c)* $\frac{1}{3}$, *d)* $\frac{1}{4}$, *e)* $\frac{1}{m}$, *f)* 0, *g)* 0, *h)* 0, *i)* 0, *j)* 0.

15. $\frac{1}{11}$.

## Sección 11.2

1. $15/(2\pi^2)$.
2. $\dfrac{6}{\pi^2}\sum_{j=1}^{10}\dfrac{1}{j^2}$.
3. $8/\pi^2$.

## Sección 11.4

1. $1/2$, $0$, $1/3$, $1/m$.

# Indice

ESTA OBRA SE TERMINO DE IMPRIMIR EL DIA 28 DE FEBRERO DE 1976, EN LOS TALLERES DE IMPRESIONES MODERNAS, S. A., SEVILLA 702, COL. PORTALES, MEXICO 13, D. F.

LA EDICION CONSTA DE 2,000 EJEMPLARES
Y SOBRANTES PARA REPOSICION

KE-100

## OBRAS AFINES:

### MANUAL DE MATEMATICAS, GEOMETRIA ANALITICA Y TABLAS MATEMATICAS
**Ralph G. Hudson y Joseph Lipka**

Este manual de tablas y fórmulas matemáticas contiene valiosísima información que resulta útil e indispensable, no sólo para usarlo en clase, sino también como libro de referencia para profesionistas en general.

Las fórmulas y tablas que abarca son las utilizadas comúnmente por los estudiantes de matemáticas e ingeniería, y están ordenadas sistemáticamente para facilitar la rápida localización del dato deseado. Las tablas numéricas se dan, por lo general, con cuatro cifras decimales, lográndose la aproximación que mejor satisface las exigencias prácticas.

### INTRODUCCION A LA MATEMATICA MODERNA
**Suger, Morales y Pinot**

La finalidad de esta obra es proporcionar al estudiante los conceptos fundamentales e indispensables para facilitar su ingreso al maravilloso Templo de la Matemática, a traves de un lenguaje actualizado, conceptos precisos y notación unificada y concisa, adecuados al razonamiento lógico deductivo característico de la misma. Además, los autores tuvieron especial cuidado en presentar la formulación clara y rigurosa del pensamiento matemático.

Por lo tanto, este es un magnífico libro de texto para el curso de Matemáticas Fundamentales que se imparte en las diversas carreras de Ingeniería y Ciencias en los centros de estudios superiores. También es una obra muy valiosa no sólo para estudiantes de preparatoria o bachillerato, sino tambien para profesores de enseñanza media.

"...una introducción brillante e interesante a la teoría de los números... El estilo es agradable y perspicaz; la motivación para las ideas y los métodos se presenta con habilidad didáctica; las definiciones son exactas; las demostraciones se establecen con seguridad... Es la creencia del crítico que este texto elemental... puede ser el mejor en su tema."

Así opina A. L. Whiteman respecto a
la primera edición en el Bulletin
of The American Mathematical Society

**ESTE TEXTO SE DESTACA** en los siguientes puntos:

°Se añadieron nuevos e interesantes problemas y se clasificaron según su grado de dificultad para lograr la transición adecuada de los fáciles a los difíciles.

°Se aclararon ciertas partes de la presentación con objeto de obtener mayor lucidez, y se reescribieron algunas demostraciones para mejorar su comprensión.

°Se incorporó nuevo material algebraico a fin de que el estudiante refuerce la comprensión de los conceptos algebraicos, y se desarrolló la teoría de la raíz primitiva tanto en el texto como en los problemas.